



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

LETECKÝ ÚSTAV

INSTITUTE OF AEROSPACE ENGINEERING

**APLIKACE TECHNIK K ZAJIŠTĚNÍ BEZPEČNOSTI A
SPOLEHLIVOSTI SOUSTAV KOSMICKÝCH PROSTŘEDKŮ**

APPLICATION OF SAFETY AND RELIABILITY ASSURANCE TECHNIQUES IN SPACECRAFT SYSTEMS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Marek Horčíčka

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Andrej Weisman

BRNO 2020

Zadání diplomové práce

Ústav: Letecký ústav
Student: **Bc. Marek Horčíčka**
Studijní program: Strojní inženýrství
Studijní obor: Stavba letadel
Vedoucí práce: **Ing. Andrej Weisman**
Akademický rok: 2019/20

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Aplikace technik k zajištění bezpečnosti a spolehlivosti soustav kosmických prostředků

Stručná charakteristika problematiky úkolu:

Průkaz zajištění bezpečnosti a spolehlivosti je nedílnou součástí návrhu soustav v kosmické technice. Požadavky na bezpečnost a spolehlivost a používané analýzy se však liší od postupů zažitých v oblasti letectví. Předmětem této diplomové práce je popsat postupy a metody zajištění bezpečnosti a spolehlivosti v kosmické technice a ověřit implementaci těchto postupů na komplexním příkladu instalace malého komerčního satelitu.

Cíle diplomové práce:

- 1) Provést rešerši dostupných standardů a souvisejících požadavků pro zajištění bezpečnosti a spolehlivosti soustav kosmických prostředků (ESA).
- 2) Zvolit a popsat vhodné postupy, metody a modely sloužící k průkazu bezpečnosti a spolehlivosti kosmických prostředků (Analýza spolehlivosti, FMECA, Analýza rizik,...), a popsat jejich specifika v porovnání s metodami a postupy používanými v oblasti letectví.
- 3) Prokázat vhodnost navržených postupů a ověřit implementaci vybraných metod na komplexním příkladu instalace malého komerčního satelitu.

Seznam doporučené literatury:

FORTESCUE, Peter W., John STARK a Graham SWINERD. Spacecraft systems engineering. 4th ed. Hoboken, N.J.: Wiley, c2011. ISBN 9780470750124.

ECSS-Q-ST-30C, Space product assurance – Dependability, February 15, 2017.

ECSS-Q-ST-40C, Space product assurance – Safety, February 15, 2017.

MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis,
November 24, 1980.

TOR-2098591-13, Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide,
June 15, 2009.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně, dne

L. S.

doc. Ing. Jaroslav Juračka, Ph.D.
ředitel ústavu

doc. Ing. Jaroslav Katolický, Ph.D.
děkan fakulty

ABSTRAKT

Práce řeší postupy zajištění bezpečnosti a spolehlivosti u kosmických prostředků. Popisuje metody a aplikuje je na příkladu malého komerčního satelitu.

ABSTRACT

Thesis is focused on safety and reliability of space products. It describes assessment methods and applies them on small commercial satellite.

KLÍČOVÁ SLOVA

Kosmická technika, spolehlivost, bezpečnost, umělá družice

KEY WORDS

Spacecraft system, dependability, reliability, safety, artifical satellite

BIBLIOGRAFICKÁ CITACE

HORČIČKA, Marek. *Aplikace technik k zajištění bezpečnosti a spolehlivosti soustav kosmických prostředků*. Brno, 2020. Dostupné také z: <https://www.vutbr.cz/studenti/zav-prace/detail/124159>. Diplomová práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Letecký ústav. Vedoucí práce Ing. Andrej Weisman.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem tuto diplomovou práci na téma *Aplikace technik k zajištění bezpečnosti a spolehlivosti soustav kosmických prostředků* vypracoval samostatně s použitím odborné literatury a pramenů uvedených v seznamu použitých zdrojů.

V Brně dne

Bc. Marek Horčíčka

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce panu Ing. Andreji Weismanovi za odborné vedení, cenné rady a vstřícnost během celé diplomové práce. Děkuji také panu doc. Ing. Jiřímu Hlinkovi, Ph.D. za ochotu, cenné rady a pedagogický pohled při vypracování diplomové práce.

Poděkovat bych chtěl i svým rodičům a přítelkyni za maximální podporu a za vytvoření ideálních podmínek pro studium.

OBSAH

ÚVOD	15
1 Základy vesmírné techniky satelitů	16
1.1 Rozdělení vesmírných satelitů	16
1.2 Zajištění produktů pro vesmírné systémy	18
2 Standardizace	20
2.1 ECSS standardizace.....	20
2.2 Vojenské standardy	22
3 Spolehlivost vesmírných prostředků	23
3.1 Analýza odlehčení součástek (derating).....	24
3.2 Analýza nejhoršího případu (Worst-Case Analysis)	26
3.2.1 Podmínky, které ovlivňují parametry součástí	26
3.2.2 Metody analýzy	28
3.2.3 Příklad provedení WCA	29
3.3 Analýza bezporuchovosti	30
3.3.1 Predikce bezporuchovosti.....	30
3.3.2 Blokové diagramy bezporuchovosti (RBD)	33
3.4 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)	36
4 Bezpečnost vesmírných prostředků.....	41
4.1 Analýza nebezpečí (Hazard Analysis)	42
4.2 Analýza stromu poruchových stavů (FTA)	46
5 Satelit UPSat	48
5.1 Rozdělení satelitu UPSat.....	49
5.1.1 Nosná konstrukce satelitu.....	50
5.1.2 Elektrický zdrojový systém (EPS).....	51
5.1.3 Systém pro získávání obrazu (IAC).....	51
5.1.4 Vědecká jednotka (SU).....	52
5.1.5 Systém určování polohy a řízení (ADCS)	52
5.1.6 Palubní počítačový systém (OBC)	52
5.1.7 Komunikační systém (COMM).....	53
6 Analýza elektrického zdrojového systému (EPS)	54
6.1 Popis a funkce systému	54
6.2 Analýza odlehčení součástek	58
6.3 Analýza bezporuchovosti	60

6.3.2 Výpočet pravděpodobnosti bezporuchového provozu sériového systému	64
6.3.3 Výpočet pravděpodobnosti bezporuchového provozu paralelního systému.....	64
6.4 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)	67
ZÁVĚR.....	71
ZDROJE	73
SEZNAM OBRÁZKŮ	76
SEZNAM TABULEK.....	77
PŘÍLOHY.....	78

ÚVOD

Zajištění bezpečnosti a spolehlivosti je nedílnou součástí návrhu soustav v kosmické technice. Cílem práce je zpracovat přehled používaných standardů sloužících k zajištění bezpečnosti a spolehlivosti soustav kosmických prostředků. Dalším cílem je na základě informací v těchto standardech zvolit vhodné metody a postupy, sloužící k průkazu bezpečnosti a spolehlivosti kosmických soustav a popsat jejich odlišnosti oproti konvenčním metodám a postupům používaným v oblasti letectví. V rámci spolehlivosti jsou to: analýza odlehčení součástí, analýza nejhorších případů, analýza bezporuchovosti a analýza způsobů, důsledků a kritičnosti poruch (FMECA). V rámci bezpečnosti jsou to: analýza nebezpečí a analýza stromu poruchových stavů.

Přehled metod a postupů je zpracován na základě standardu ECSS. Pro malé satelity se obvykle neaplikují metody k zajištění bezpečnosti v takové míře a takovým způsobem, jak je to obvyklé v oblasti civilního letectví, a to z důvodu absence letové posádky. Z toho důvodu je oblast zajištění bezpečnosti v diplomové práci zmíněna pouze okrajově a hlavní část práce se zaměřuje na popis spolehlivostních metod. Mezi analýzy, které byly vybrány jako vhodné k aplikaci pro malý komerční satelit patří: analýza odlehčení součástí, analýza bezporuchovosti a analýza způsobů, důsledků a kritičnosti poruch (FMECA). Analýzy na sebe navazují a postupně ukazují proces ověření správnosti návrhu obvodu elektrického zdrojového systému nanosatelitu UPSat s použitím spolehlivostních metod.

1 Základy vesmírné techniky satelitů

Vesmírnou družicí se označuje objekt, který se pohybuje po oběžné dráze jiného hmotnějšího tělesa. Družice mohou být z hlediska jejich původu přírodní nebo umělé. Mezi přírodní patří například Země a Měsíc. Tato diplomová práce se zaměřuje na družice umělé, které jsou vytvořeny člověkem. Umělé družice bývají často označovány také jako satelity. K prvnímu úspěšnému vypuštění satelitu do vesmíru došlo v roce 1957 Sovětským svazem (Sputnik 1). Od té doby byly do vesmírného prostoru vypuštěny tisíce satelitů. Satelity jsou využívány různými způsoby. Jsou využívány v oblasti monitorování počasí, podnebí či okolního i vzdáleného vesmírného prostoru. Dále se využívají ke komunikaci (televizní signál nebo telefonní hovory), vědecké činnosti a v rámci navigačních systémů. [43]

Jednou z největších výhod vesmírných satelitů oproti pozemním zařízením je výška, ve které pracují. Umožňují tak sledovat a monitorovat mnohem větší plochu obíhaného tělesa a získávají tak rychleji mnohem větší množství dat. Při zkoumání vesmíru je jejich viditelnost lepší než v případě pozemních teleskopů, kterým může viditelnost komplikovat zakřivení Země, znečištění atmosféry nebo mraky. [43]

1.1 Rozdělení vesmírných satelitů

Vzhled satelitů bývá často rozmanitý, co se velikosti, hmotnosti a tvaru týče. Satelity mohou mít hmotnost v řádu jednotek kilogramů až po několik tun, viz Tab.1. [20] Přesto jsou často u satelitů zaznamenávány alespoň některé společné znaky, jako jsou například zdroj elektrického napájení využívající solární panely a baterie, vysokovýkonná anténa pro komunikaci a zasílání dat na Zem, navigační systém a vědecké vybavení. [43]

Tab. 1 Kategorie satelitů podle jejich hmotnosti [20]

Velikostní kategorie satelitu	Hmotnost [kg]
Konvenční velký satelit	> 1000
Konvenční malý satelit	500 - 1000
Minisatelit	100 - 500
Mikrosatelit	10 - 100
Nanosatelit	1 - 10
Pikosatelit	< 1

Satelity jsou nejčastěji umísťovány na své oběžné dráhy pomocí vesmírných raket. [43]

Se zvyšující se výškou oběžné dráhy, po které se satelity pohybují, od povrchu Země zároveň klesá jejich rychlost. Některé satelity tak dokážou Zemi oběhnout během několika desítek minut a u jiných bude časová doba v řádu hodin i dní. Nejvíce satelitů se nachází v oblasti nízké oběžné dráhy. [37]



Obr. 1 Přehled hmotností některých satelitů [33]

Vzhledem k výšce, po které se satelit pohybuje, rozeznáváme tyto základní typy oběžných drah Země: [37]

- Nízká oběžná dráha (LEO)
- Střední oběžná dráha (MEO)
- Vysoká oběžná dráha (HEO)
- Geostacionární dráha (GEO)

LEO (180 – 2 000 km)

Jedná se o nejnižší oběžnou dráhu. Díky tomu jsou zde nejvhodnější podmínky pro snímání plochy Země v nejvyšším rozlišení. To s sebou nese i nevýhody v podobě často nedostatečně velkého pokrytí plochy Země. Satelity tak musí pracovat jako velké skupiny (konstelace), aby bylo zajištěné dostatečné pokrytí snímané plochy Země. Satelity obíhající na nízké oběžné dráze se pohybují obrovskou rychlostí, a proto vyžadují kvalitní komunikační pozemní zařízení a antény. Z toho důvodu nejsou příliš vhodné pro telekomunikační využití. Na nízké oběžné dráze obíhá i Mezinárodní vesmírná stanice (ISS) [16]. Družice na nízkých oběžných drahách jsou rovněž lépe chráněny před kosmickým zářením Zemským magnetickým polem. Negativem je velký výskyt vesmírného odpadu právě na nízké běžné dráze. [28]

MEO (2000 - 35 780 km)

Střední oběžná dráha zasahuje do poměrně rozsáhlé oblasti výšek (2000 – 35 780 km), ovšem nejvíce využívaná je oblast kolem 20000 km nad Zemským povrchem. V této výšce je oběžná doba satelitu přibližně 12 hodin a Země oběhne 2x v průběhu jednoho dne. Velmi často jsou satelity na střední oběžné dráze využívány pro navigaci. Nachází se zde družice nejznámějších navigačních systémů GPS, GLONASS nebo GALILEO [28]. Mezi významné střední oběžné dráhy patří Molniya nebo semi-synchronní oběžná dráha. [37]

GEO (35 780 km)

Ve výšce přibližně kolem 36 000 km nad povrchem Země je úhlová rychlost pohybu družic stejná jako úhlová rychlost otáčení Země kolem své osy. Družice se tak stále nachází na stejném místě nad povrchem Země. Tato výška je vhodná k monitorování počasí, protože satelit sleduje neustále stejnou plochu. Mezi další využití patří přenos televizního signálu [22]. Vynášení zejména příliš těžkých družic na geostacionární oběžnou dráhu je obtížné. Z toho důvodu se využívá dráha přechodná ke geostacionární (GTO). Družice jsou tedy umístěny na eliptickou dráhu s nejvyšším bodem ve stejné výšce, ve které se nachází geostacionární oběžná dráha. Družice pak pomocí motorů provede manévr, kdy jednak zakulatí svoji dráhu a zároveň sníží její sklon na 0°. Nejvýhodnější pozicí pro starty nosných raket je oblast v blízkosti Zemského rovníku. V oblastech dál od rovníku je nutné k dosažení GEO velké množství zážehů motoru. [28]

HEO (> 35 780 km)

Oběžná dráha nacházející se za geostacionární oběžnou dráhou nemá příliš velké využití a často se používá pouze jako odkladiště pro nepotřebné družice po skončení jejich plánované doby životnosti. Částečně se však dá využívat například pro monitorování počasí. [28]

1.2 Zajištění produktů pro vesmírné systémy

Na rozdíl od většiny ostatních forem inženýrství existují v oblasti návrhu kosmických produktů značné odlišnosti. Je zde hned několik faktorů, které je mohou ohrožovat: velmi vysoká teplota, vibrace, zrychlení, vliv vakua, kosmická radiace atd. Až na pár výjimek není většina satelitů udržovatelná. Pouze u některých finančně náročných projektů se na palubu navzdory navýšení hmotnosti přidává záložní vybavení. Pro dosažení maximální spolehlivosti a bezpečnosti se využívají nejkvalitnější materiály a nejefektivnější výrobní postupy. Materiály a součástky musí přetrvávat funkční bez přerušení po celou dobu trvání mise (až desítky let) v prostředí plném teplotních změn, radiace a vakua. [20]

Tab. 2 uvádí přehled požadavků na spolehlivost u vesmírných prostředků. Cílem je poukázat na způsob, jakým jsou požadavky na bezporuchovost uváděny v porovnání s požadavky používanými v letectví. V oblasti letectví jsou požadavky na pravděpodobnost nastoupení poruchy vztaženy vždy na jednu letovou hodinu. V oblasti vesmírných projektů, kdy mise trvají často až několik let, jsou podobně jako v oblasti vojenských aplikací požadavky na pravděpodobnost správné funkce systému vztaženy k době trvání mise. [16]

Pro dosažení maximální efektivity, šetření energie a snižování hmotnosti se používají nejmodernější technologie. Všechny jednotlivé elementy musí být způsobilé pro dané použití v daném prostředí. Každá nová navržená část musí nutně projít kvalifikační způsobilostí. [20]

Zajištění způsobilosti produktů je definováno jako disciplína, která se věnuje studiu, plánování a provádění činností, jejichž cílem je zajistit, aby návrh, kontrola, metody a techniky použité ve vesmírném projektu vedly k dostatečně uspokojivé úrovni kvality. Inženýrská oblast zabývající se zajištěním produktů určuje spolehlivostní odhady s použitím schválených standardů, hodnocení chyb nebo testovacích metod. [20]

Tab. 2 Specifikace pravděpodobnosti splnění mise [17]

Projekt	Typ mise	Délka mise [let]	Požadovaná pravděpodobnost splnění mise [%]
Cryosat 2	Sledování Země	3,5 let	70
Meteosat 2. gen.	Sledování Země	7 let	68
Meteosat 3. gen.	Sledování Země	8,5 let	75
Rosseta	Vědecký výzkum	11 let	93
Sentinel 1	Sledování Země	7 let	80
Sentinel 2	Sledování Země	7 let	70
Sentinel 3	Sledování Země	7 let	75
SEOSat	Sledování Země	7 let	65

2 Standardizace

V dřívějších dobách existovalo v Evropě více typů standardů, kterými se řídil produktový management v oblasti kosmonautiky. Kvůli snadnější a přehlednější orientaci ve standardech došlo v roce 1994 k hromadnému sjednocení do systému standardů ECSS (Evropská spolupráce pro standardizaci v oblasti kosmických aktivit). Cílem bylo vytvoření systému jednotných standardů, které by s sebou přineslo několik výhod, jako např. výhodnější cenové podmínky v kosmických programech a projektech, konkurenceschopnost evropského kosmického průmyslu, zvyšování kvality a spolehlivosti, jednodušší komunikaci mezi stranami zájmu a kompatibilitu produktů. ECSS standardy fungují závazně pouze v rámci smluv, pokud je na ně požadavek. [4]

2.1 ECSS standardizace

ECSS standardy se dělí na čtyři základní větve: management vesmírného projektu (space project management), zajištění vesmírného produktu (space product assurance), vesmírné inženýrství (space engineering) a vesmírná udržitelnost (space sustainability). Každá z těchto větví se zabývá příslušnou problematikou. [4]

Systém standardů ECSS obsahuje tyto hlavní typy dokumentů: standardy, příručky a technická memoranda. Příručky a technická memoranda obsahují pouze doplňující a rozšiřující informace ke standardům, nejsou závazné a existují pouze v některých oblastech. Označení dokumentů ECSS je normované. [4]

Formát označení: [4]

ECSS-X-YY-číslo-verze

kde:

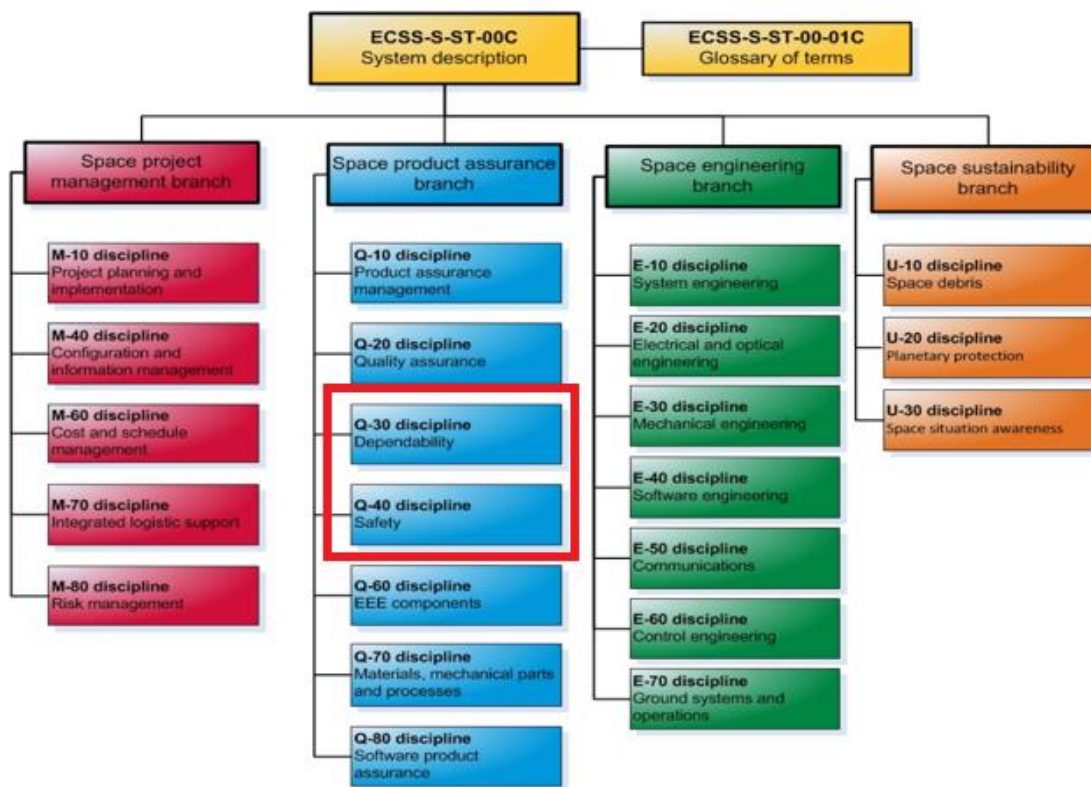
X - označuje odvětví standardů (P/S obecně pro ECSS systémy, M pro management, E pro inženýrství, Q pro zajištění produktů, E pro udržitelnost)

YY - označuje typ dokumentu (ST pro standardy, HB pro příručky, TM pro technická memoranda)

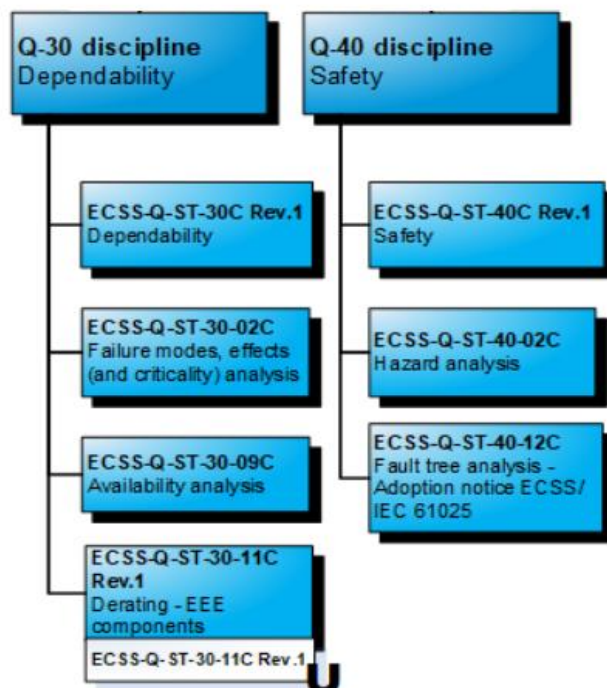
číslo a verze - označují specificky konkrétní dokumenty

Např. označení ECSS-Q-ST-30-02C odkazuje na ECSS dokument, odvětví zajištění produktu, typ dokumentu je standard pro oblast spolehlivosti. Označení 02C reprezentuje konkrétní číslo pro metodu FMEA/FMECA.

Pro oblast řešení spolehlivosti a bezpečnosti kosmických prostředků je nejvýznamnější větev týkající se zajištění produktů Q-30 a Q-40. Cílem je zajistit spolehlivou a bezpečnou funkci kosmických produktů vedoucí k úspěšnému splnění mise. V diplomové práci tak bude věnována pozornost pouze spolehlivostní a bezpečnostní disciplíně ve větví zabývající se zajištěním produktu. Spolehlivost a bezpečnost jsou na sebe velmi často navázány a metody uvedené v této práci se mohou využívat v obou disciplínách. Rozvržení kapitol a zařazení jednotlivých metod bylo v práci bylo provedeno především na základě struktury a větvení standardů ECSS viz. Obr.3.



Obr. 2 Rozdělení disciplín podle ECSS [7]



Obr. 3 Rozdělení větve spolehlivosti a bezpečnosti [7]

2.2 Vojenské standardy

Kromě již uvedených vesmírných standardů je nutno uvést rovněž standardy vojenské (Military), a to z důvodu, že některé z nich byly využity při zpracování diplomové práce. Jedná se o vojenské standardy a specifikace vydávané ministerstvem obrany USA. Značná část těchto dokumentů se zaměřuje také na oblast spolehlivosti a bezpečnosti. Uplatnění těchto norem není pouze v oblasti vojenských projektů, ale jsou vzhledem k jejich přehlednosti oblíbené také v ostatních průmyslových odvětvích. Zpracování norem ve formě podrobných návodů je velmi nápomocné pro jejich aplikaci. [19]

Tab. 3 Základní rozdělení vojenských dokumentů [19]

Typ dokumentu	Specifikace
MIL-HDBK (Defense Handbook)	Průvodní dokument obsahující technické, inženýrské a návrhové informace
MIL-SPEC (Defense Specification)	Dokument, který popisuje technické požadavky pro zakoupené vojenské nebo modifikované komerční materiály
MIL-STD (Defense Standard)	Dokument, který stanovuje požadavky na vojenské nebo jinak modifikované komerční procesy, postupy a metody
MIL-PRF (Performance Specification)	Dokument uvádí požadavky z hlediska požadovaných výsledků včetně kritérií pro ověření shody
MIL-DTL (Detail Specification)	Dokument specifikuje detailní konstrukční a návrhové požadavky

3 Spolehlivost vesmírných prostředků

U vesmírných produktů je žádoucí dosažení vysokých pravděpodobností správné funkce a minimalizování nebo eliminování vzniku poruch, které mohou vést k poruše produktu. [20]

Vesmírné mise narozdíl od použití v letectví mají často dobu kontinuálního provozu v řádu několika let. Proto je jedním z nejdůležitějších cílů zajištění spolehlivosti a správné funkce produktu po dobu trvání mise. [16] Spolehlivost zahrnuje tyto technické disciplíny: [5]

- bezporuchovost – „Schopnost fungovat v daných podmínkách během daného časového intervalu bez poruch tak, jak je požadováno.“
- pohotovost – „Schopnost objektu být ve stavu, kdy funguje tak, jak je požadováno.“
- udržitelnost - „Schopnost objektu v daných podmínkách používání a údržby být udržen ve stavu nebo navrácen do stavu, kdy funguje tak, jak je požadováno.“

Snaha o zajištění lepší spolehlivosti jde vždy na úkor ostatních požadavků jako jsou hmotnost, cena, zabezpečení atd. Vhodným příkladem je například velmi často používaná redundance kritických funkcí, čímž však narůstá hmotnost produktu. V rámci ESA musí být spolehlivost a bezpečnost zajišťována jak u satelitů samotných, tak i u pozemní infrastruktury. [16]

Nutno mít na paměti, že u vesmírných misí neexistuje druhá šance. V případě špatného návrhu produktu může jednoduše dojít k poruchám, které jsou neopravitelné a mohou mít významný finanční důsledek. Uvedený problém tak spolu se současnými trendy a technologickým vývojem přináší novou úroveň náročnosti pro spolehlivost. [16]

Kosmický průmysl na rozdíl od leteckého obvykle nemůže postupovat podle principu fly-fix-fly. U vesmírných programů se očekává, že budou fungovat jednorázově a budou tedy muset plnit přísné požadavky na pravděpodobnost splnění mise. Jen výjimečně se využívá servisních misí na satelitech již umístěných na oběžné dráze (ISS, Hubbleův teleskop). [16]

Spolehlivost se tak stává zásadním aspektem každého kosmického projektu a je klíčová v hodnocení celkové kvality konečného produktu. Předchozí zkušenosti ukazují, že dostatečné zajištění spolehlivosti a bezpečnosti je vždy méně investičně nákladné než případné selhání mise. [16]

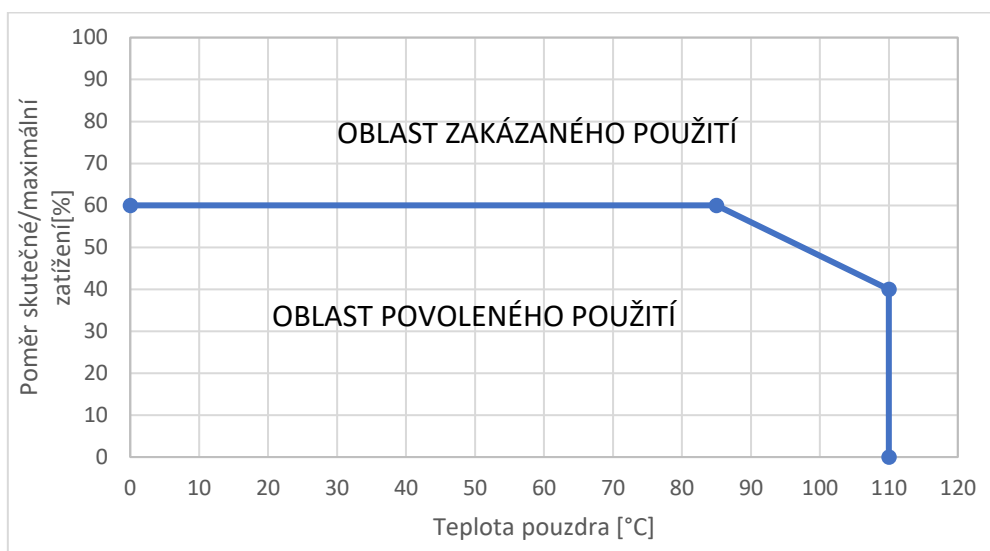
Systém standardů ECSS definuje program zajištění spolehlivosti a veškeré spolehlivostní požadavky pro vesmírné systémy. Program zajištění spolehlivosti je nepřetržitý, který se opakuje v průběhu celého životního cyklu projektu. Spolehlivost dle standardů ECSS je založena na aplikaci programu zajištění spolehlivosti, který se skládá z: [9]

- Zjištění všech technických rizik s ohledem na funkční potřeby, které mohou vést k nedodržení spolehlivostních požadavků.
- Použití analýzy a jiných metod pro zjištění, zda jsou spolehlivostní cíle splněny.
- Optimalizace celkových nákladů a plánování s důrazem na to, že:
 - pravidla návrhu, analýzy spolehlivosti a možnosti snížení rizik odpovídají definovaným kategoriím závažnosti.
 - možnosti snížení rizik jsou realizovány nepřetržitě od počáteční fáze projektu.
- Vstupu do sériové produkce.

3.1 Analýza odlehčení součástek (derating)

Odlehčení tzv. derating je záměrné snižování elektrických, teplotních nebo mechanických parametrů na součástkách pod úroveň jejich maximálního přípustného zatížení. Účelem je snížení pravděpodobnosti nástupu poruchy a zvýšení životnosti a spolehlivosti součástky. Důvody, kvůli kterým se metoda deratingu používá, mohou být neočekávané výkyvy zatížení nebo různé tolerance parametrů součástek. [12] Jedná se o obdobu používání součinitelů bezpečnosti v návrhu mechanických konstrukcí.

Příkladem může být napěťové odlehčení keramického kondenzátoru. Cílem je zajistit, aby se skutečné provozní hodnoty napětí vyskytovaly v oblasti povoleného napětí pod křivkou. Tím by mělo být zajištěno, že i v případě nečekaných výkyvů daného parametru při provozu nedojde k překročení maximálních konstrukčních hodnot a následné poruše součástky.



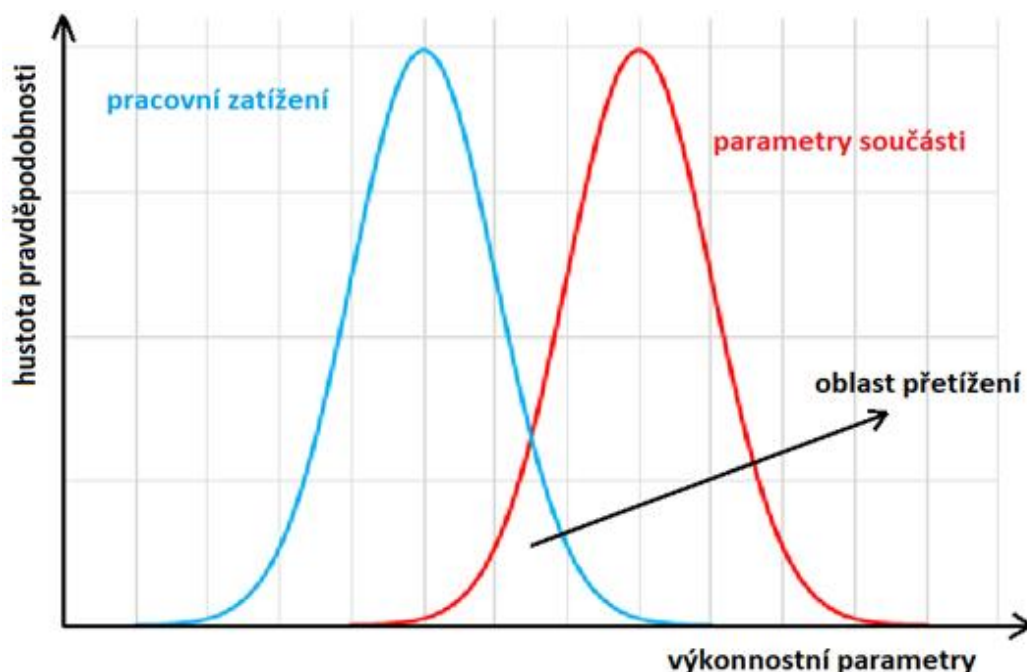
Obr. 4 Odlehčení napětí keramického kondenzátoru [12]

Derating elektrických, elektronických a elektromechanických součástek se používá v řádu desítek let. Podstatným úkolem je však nalezení optimální spolehlivosti produktu bez extrémního navýšení rozměrů a ceny produktu. Standard ECSS-Q-ST-30-11C definuje detailní požadavky na derating elektrických, elektronických a elektromechanických součástek v závislosti na parametrech okolního prostředí. [12]

Základní princip deratingu vyplývá z variability parametrů součástky. Ty mohou být ovlivněny výrobcem, typem součástky, kvalitou součástky atd. Výsledkem je obvykle statistická křivka hustoty pravděpodobnosti podléhající Gaussovu normálnímu rozdělení. Podobně je to i s pracovním zatížením součástky, které je opět proměnné v závislosti na okolních podmínkách (vibrace, teplota...). Vzniká tak další statistický soubor. K lepší interpretaci a vysvětlení principu deratingu je velmi nápomocný Obr. 5. Součástka pracuje spolehlivě v případě, že červená křivka (parametry součástky) se nachází vpravo od modré křivky (pracovní zatížení). Oblast pod průsečíkem obou křivek reprezentuje možný výskyt poruchy. Se zvětšující se společnou oblastí se zvyšuje také pravděpodobnost nástupu poruchy. Úkol tak spočívá ve zmenšení daného průsečíku a nadimenzování parametrů součástky tak, aby výskyt poruchy nebyl příliš velký, a zároveň, aby nedošlo k zbytečnému předimenzování těchto parametrů. [12]

Logicky se zde nachází dvě možnosti, jak toho dosáhnout: [12]

- Snížení pracovního zatížení součástky (posun modré křivky doleva)
- Zvýšení výkonnostních parametrů součástky (posun červené křivky doprava)



Obr. 5 Vztah pracovního zatížení a parametrů součásti [12]

Spolehlivost elektronických součástí je závislá nejen na elektrickém namáhání ale i na teplotním. Při vzrůstu okolní teploty dochází rovněž ke zvyšování vnitřní teploty součástky, což má negativní vliv na hodnotu intenzity poruchy. Spolehlivost některých součástí tedy může být výrazně negativně ovlivněna teplotním zatížením (především polovodiče). Parametry, které jsou odlehčovány závisí na typu analyzované součástky. [13] Mezi hlavní odlehčované parametry patří např. teplota pouzdra, teplota přechodu, proud, napětí, parametry výkonu. [12]

Tab. 4 Odlehčované parametry součástek dle typu součástek [32]

Typ součástky	Parametr součástky			
	Teplota	Napětí	Proud	Výkon
Kondenzátor	X	X		
Dioda	X	X	X	X
Cívka	X	X		
Rezistor	X	X		X
Integrovaný obvod	X	X	X	X
Tranzistor	X	X	X	X
X - označuje parametry, u kterých se provádí odlehčování				

3.2 Analýza nejhoršího případu (Worst-Case Analysis)

Vesmírné systémy musí být navrženy tak, aby pracovaly s maximální spolehlivostí po celou dobu své životnosti. Z tohoto důvodu je nutné mít znalosti o výkonnosti navrhovaného systému v případě, že se parametry součástek změní z důvodu vlivů okolního prostředí, jako např. teplota, vlhkost, elektrické zatížení, vesmírná radiace, stárnutí. [25]

Analýza nejhoršího možného případu tedy určuje chování a výkon obvodu za nejhorších možných okolních podmínek s uvažováním variability součástek. Cílem je dosažení vysoké pravděpodobnosti správné funkčnosti i v případě, že se všechny parametry všech součástí dostanou do extrémně nepříznivých hodnot. Nejhorší podmínky se dělí na podmínky prostředí a provozní podmínky. Mezi podmínky prostředí, které jsou definovány jako vnější působení na části obvodu, patří teplota, vlhkost, radiace atd. Provozními podmínkami se rozumí například externí elektrické vstupy, kvalita součástek a jejich vzájemné působení nebo stárnutí materiálu. Analýza napomáhá k odhalení problému návrhu vesmírného produktu v časných fázích. To vede ke snížení pravděpodobnosti problémů spolehlivosti, bezpečnosti a finančních rizik. [25,36]

3.2.1 Podmínky, které ovlivňují parametry součástí

- Počáteční tolerance (např. výrobní)
- Teplota
- Stárnutí
- Radiace
- Vlhkost
- Ostatní

Provozní nebo okolní podmínky, které nejvíce ovlivňují součástky se liší právě s typem součástky. Podmínka, která může velmi ovlivňovat parametry jedné součástky, nemusí mít tak velký vliv na součástku jiného typu. Každá součástka má předurčené vlastní podmínky, se kterými se musí počítat. V Tab. 5 je uveden příklad některých součástek a podmínek, které je nejvíce ovlivňují. [25]

Tab. 5 Ovlivnění parametrů součástek podmínkami okolí [36]

	Tranzistor	Kondenzátor	Rezistor	Cívka
Teplota	X	X	X	X
Stárnutí	X	X	X	X
Radiace	X			
Vlhkost		X	X	
X – označuje podmínky, které ovlivňují parametry dle typu součástky				

Provedení analýzy poskytuje návrhářům systému cenné informace o vlivu variability součástek na výkonost celého obvodu. Potřebná identifikace a kvalifikace variability následně napomáhá

k lepší kontrole a řízení návrhu obvodu. Výstupem analýzy je umožněno porovnání skutečných charakteristických hodnot součástek při nejhorším scénáři oproti hodnotám nominálním. [38]

V klasickém přístupu se uvažuje se správnou funkčností za ideálních podmínek. Podmínky variability prostředí a parametrů nejsou v průběhu návrhu zvažovány. Analýza nejhorších případů však počítá s tím, že se veškeré podmínky nachází v nejhorším možném stavu. Podmínky jsou tak zahrnuty přímo v analýze a ta je prováděna za takto přísných podmínek. Výsledná analýza nám s jistotou zajišťuje správnou funkci obvodu i při nastoupení nejhoršího možného scénáře. Avšak to, že by daný scénář opravdu nastal je vysoce nepravděpodobné. [25,36]

Z časových nebo finančních důvodů se analýza neprovádí na celém obvodu, ale pouze na kritických místech. Dále může rozsah analýzy ovlivňovat dostupnost nástrojů a dat pro analýzu. Jedním z nejdůležitější a nejvíce kritických kroků je dostupnost databáze parametrů součástek. Tato databáze obsahuje informace ohledně variability parametrů součástek. Pomocí ní je možné vyvodit nejhorší možné scénáře pro parametry součástek. Dalším potřebným krokem je získání i druhé části dat, podmínky prostředí. Jako zdroje databází se nejčastěji používají: [36,38]

- Firemní databáze
- Databáze agentur (ESA)
- Databáze výrobců
- Vojenské databáze
- Ostatní zdroje

V databázích jsou obsaženy informace o variabilitě parametrů součástek vlivem okolních nebo provozních podmínek nejčastěji ve formě tolerancí. Pro výpočty se rozlišují dva typy tolerančních hodnot: [8]

- ovlivněné (bias) - pokud se dá předpokládat, kterým směrem se bude toleranční hodnota ubírat. Nejčastěji se používá u podmínek prostředí (teplota, radiace, stárnutí), kdy se dá předpovídat směr odchylky parametru
- náhodné (random) - hodnota nemá známý směr, kterým se bude ubírat. Nejčastěji se používá u počátečních (výrobních) tolerancí, ale může být použita i u ostatních

Ovlivněná složka je odvozena algebraicky a pro náhodnou složku se využívá Gaussova rozdělení s rozptylem 3σ . [36]

Tab. 6 Typ používaných tolerančních hodnot podle ovlivňujících podmínek [8]

Podmínky ovlivňující parametry součásti	Počáteční tolerance	Stárnutí	Teplota	Radiace
Typ toleranční hodnoty	Náhodná	Ovlivněná (může být i náhodná)	Ovlivněná (může být i náhodná)	Ovlivněná (může být i náhodná)

V Tab. 7 je jako příklad uveden vliv stárnutí na toleranční hodnoty. Typ tolerančních hodnot je v tomto případě náhodný, jelikož si jsou kladná i záporná (\pm) odchylka rovny. Např. tolerance hodnot kapacity tantalového kondenzátoru s předpokládanou funkční dobou 18 let při teplotě 110 °C bude vlivem stárnutí $\pm 3 \%$. Podobným způsobem by bylo možné zjistit i toleranční hodnoty vlivem ostatních okolních nebo provozních podmínek a zjistit výslednou toleranční hodnotu daného kondenzátoru pomocí některé z metod analýzy nejhorších případů.

Tab. 7 Příklad vlivu stárnutí na parametry [15]

El. Kapacita $\Delta C/C$	55 °C	85 °C	110 °C
10 let	$\pm 0,63 \%$	$\pm 1,11 \%$	$\pm 1,67 \%$
18 let	$\pm 1,14 \%$	$\pm 2 \%$	$\pm 3 \%$

3.2.2 Metody analýzy

Elektronické obvody jsou vytvořeny z různých typů součástek o různých parametrech. Všechny komponenty však nejsou ideální a jejich skutečné hodnoty se mohou měnit vlivem okolního prostředí. Musíme počítat s důsledky výrobních tolerancí, pracovního prostředí, stárnutí a pro vesmírné prostředí také radiace. Jednotlivé součástky tak mohou mít různé parametry právě vlivem výše zmíněných důsledků. [25]

Pro zpracování analýzy nejhorších případů se nejčastěji používá některá ze tří metod: [25]

- EVA (Extreme Value Analysis) – Analýza extrémních hodnot
- RSS (Root-Sum-Squared)
- Monte Carlo Analysis

EVA - Metoda patří mezi nejzákladnější a nejjednodušší. Je vhodná především pro počáteční vstup a odhad variability. Její pesimistický přístup počítá právě s extrémně nejnepríznivějšími hodnotami. Na jednu stranu zajišťuje, že v případě úspěšné analýzy bude zaručena spolehlivost celého obvodu, a tudíž není nutné používat některou z dalších metod. Na druhou stranu situace, že ve skutečnosti nastane nejhorší možný scénář pro všechny součástky najednou je vysoce nepravděpodobná. Využití této metody není příliš vhodné, a to z důvodu nastavení velkého rozmezí hodnot obvodu. Výpočet rozmezí těchto hodnot spočívá v přičtení pozitivních efektů a odečtení efektů negativních od nominální hodnoty. [25]

Tab. 8 Výpočet hodnot WCA podle metody EVA [38]

Extreme Value Analysis (EVA)	$\text{Min}_{\text{EVA}} = \text{Nominální hodnota} - \sum (\text{Negativní efekty})$ $\text{Max}_{\text{EVA}} = \text{Nominální hodnota} + \sum (\text{Pozitivní efekty})$
-------------------------------------	---

RSS - Ve srovnání s EVA se jedná o složitější, více optimistickou a realistickou metodu. Metoda využívá statistického přístupu. Využívá předpokladu, že při nastání extrému u jednoho z parametrů součástky se velmi často všechny ostatní parametry do extrémně kritických hodnot nedostanou. [25]

Tab. 9 Výpočet hodnot WCA podle metody RSS [38]

Root-Sum-Squared (RSS)	$\text{Min}_{\text{RSS}} = \text{Nominální hodnota} - \sum \text{Neg. bias} - \sqrt{\sum (\text{Náhodná složka})^2}$ $\text{Max}_{\text{RSS}} = \text{Nominální hodnota} + \sum \text{Poz. bias} + \sqrt{\sum (\text{Náhodná složka})^2}$
-------------------------------	---

Monte Carlo - Ze všech tří metod se jedná o metodu nejvíce realistickou, ale zároveň nejvíce složitou pro použití. Nutností je využití počítače. Metoda využívá náhodného výběru hodnot parametrů součástek a následné analýzy obvodu s danými součástkami. Pro dosažení

věřitelných výsledků je nutné provedení mnohonásobného iteračního procesu. Obvyklá hodnota počtu iterací se pohybuje v řádu tisíců, ale při využití výkonného počítače může být i mnohonásobně vyšší. [36]

3.2.3 Příklad provedení WCA

Průběh analýzy a výpočtů bude demonstrován na kondenzátoru s kapacitou 10uF. Pro daný kondenzátor je nutné zjistit z databáze počáteční toleranční hodnoty a toleranční hodnoty způsobené podmínkami okolí viz. Tab.10. WCA bude provedena a spočítána pomocí metod EVA a RSS.

Tab. 10 Příklad ovlivněných a náhodných tolerančních hodnot kondenzátoru [38]

Parametr	Ovlivněné (bias)		Náhodné (random)
	Neg.	Poz.	
Počáteční tolerance	---	---	± 10 %
Teplota	---	---	± 15 %
Napětí	- 12,5 %	+ 7,5 %	---
Stárnutí	---	---	± 8,7 %

- **EVA**

Výpočet pozitivních a negativních efektů:

$$\sum \text{Pozitivních efektů} = 10 + 15 + 7,5 + 8,7 = 41,2 \% \quad (3.1)$$

$$\sum \text{Negativních efektů} = 10 + 15 + 12,5 + 8,7 = 46,2 \% \quad (3.2)$$

Výpočet maximální a minimální odchylky kapacity kondenzátoru podle Tab. 8:

$$\text{Max } C_{EVA} = 10 + 4,12 = 14,12 \text{ uF} \quad (3.3)$$

$$\text{Min } C_{EVA} = 10 - 4,62 = 5,38 \text{ uF} \quad (3.4)$$

- **RSS**

Výpočet ovlivněných a náhodných tolerančních hodnot

$$\sum \text{Pozitivních ovlivněných hodnot} = 7,5\% \quad (3.5)$$

$$\sum \text{Negativních ovlivněných hodnot} = 12,5 \% \quad (3.6)$$

$$\sqrt{\sum (\text{Náhodných složek})^2} = \sqrt{10^2 + 15^2 + 8,7^2} = 20 \% \quad (3.7)$$

Výpočet maximální a minimální odchylky kapacity kondenzátoru podle Tab. 9:

$$\text{Max } C_{RSS} = 10 + 0,75 + 2 = 12,75 \mu F \quad (3.8)$$

$$\text{Min } C_{RSS} = 10 - 1,25 - 2 = 6,75 \mu F \quad (3.9)$$

Na daných výsledcích lze vidět výrazný rozdíl rozptylu hodnot při použití metod EVA a RSS. V případě EVA metody, která zvažuje opravdu nejhorší možný scénář a tím zaručuje správnou funkci je rozptyl hodnot kapacity kondenzátoru větší než u metody RSS, která je naopak více realističtější.

3.3 Analýza bezporuchovosti

Analýza bezporuchovosti poskytuje kvantitativní parametry potřebné pro posouzení úrovně spolehlivosti produktu. Odhad inherentní spolehlivosti nových produktů především před jich produkcí, ale i během ní, je velice důležitý. Za pomoci získaných odhadů lze s předstihem rozhodovat o vhodnosti konceptu, volbě úrovně kvality součástek a dalších faktorů. Použitím predikcí a modelů bezporuchovosti lze odhalit vhodnost navrženého prvku, aby splňoval zadané požadavky. [32,34]

Analýza bezporuchovosti je tvořena: [32]

- Predikcí bezporuchovosti (odhady intenzit poruch nebo ekvivalentních parametrů)
- Modely bezporuchovosti (Blokové diagramy bezporuchovosti a jejich matematické reprezentace)

3.3.1 Predikce bezporuchovosti

Predikce bezporuchovosti slouží k ověření proveditelnosti specifikovaných požadavků. Požadavky na bezporuchovost jsou většinou přísnější pro dlouho trvající nebo finančně náročné mise. U krátkodobých misí, s menší mírou důležitosti a ceny jsou většinou jediné požadavky na odstranění kritických oblastí a použití komponent s úrovní kvality pro používání ve vesmíru. Postupně se predikce bezporuchovosti aplikuje od nejnižší úrovně (součástky), až po vyšší úrovně (subsystémy, samotný systém). U vesmírných zařízení je většina komponentů elektrická nebo elektronická. Jako hlavní ukazatel bezporuchovosti se používá intenzita poruch, která je definována jako očekávaný počet poruch objektu za určitý časový interval. Většinou se intenzita poruch udává v počtu poruch za milion hodin. [21] Nejčastěji se pro predikci bezporuchovosti elektrických a elektronických komponent využívá vojenská příručka bezporuchovosti MIL-HDBK-217F, ve které se pracuje s modely pro výpočet bezporuchovosti. V daných modelech je výpočet intenzity poruch ovlivněn pracovním prostředím, kvalitou součástky, teplotou a podle typu součástky i dalšími faktory. [17]

Používané základní modely pro výpočet intenzity poruch podle příručky MIL-HDBK-217F [31] pro:

- Integrované obvody

$$\lambda_p = (C_1\pi_T + C_2\pi_E) \pi_Q\pi_L, \quad \text{poruch}/10^6h \quad (3.10)$$

kde je λ_p intenzita poruch součástky, π_T je součinitel teploty, π_Q je součinitel kvality součástky, π_E je součinitel prostředí, π_L je součinitel zkušenosti, C_1 a C_2 jsou součinitele složitosti integrovaného obvodu. [31]

- Ostatní součástky

$$\lambda_p = \lambda_b\pi_T\pi_A\pi_R\pi_S\pi_C\pi_Q\pi_E, \quad \text{poruch}/10^6h \quad (3.11)$$

kde je λ_p intenzita poruch součástky, λ_b je základní intenzita poruch, π_Q je součinitel kvality součástky, π_E je součinitel prostředí. Součinitele π_Q a π_E jsou využívány u téměř všech typů součástek. Ostatní zmíněné součinitele π jsou používány pouze pro konkrétní typy součástek. [31]

Jak bylo zmíněno, na výslednou intenzitu poruch má zásadní vliv úroveň kvality součástky. Většina vyrobených součástek má jasně deklarovanou úroveň kvality. Tato úroveň odpovídá hodnotě faktoru kvality π_Q , která ovlivňuje výslednou intenzitu poruchy. Úrovně kvality se mohou lišit podle typu součástek. Příklad úrovní kvality některých vybraných součástek podle vojenských standardů je v Tab. 10. [31]

Tab. 10 Označení úrovně kvality součástek dle vojenských standardů (MIL) [31]

Typ součástky	Úroveň kvality
Polovodič	JANTXV, JANTX, JAN
Kondenzátor	D, C, S, R, B, P, M, L
Rezistor	S, R, P, M

Různé příručky používají různé označení úrovně kvality. Je-li označení úrovně kvality součástky definována dle jiné příručky, je nutné dohledat ekvivalentní označení.

Tab. 11 Převodová tabulka úrovně kvality součástek [11]

Úroveň kvality			
	kategorie S	kategorie B	kategorie B1
Aktivní součástky	MIL JAN třída S	MIL JAN třída B	MIL 883 B
	MIL QML třída V	MIL QML třída Q	MIL QML třída M, N, T
	MIL QML třída K	MIL QML třída H	MIL QML třída D, E
	MIL JANS	MIL JANTXV a JANJ	MIL JANTX a JAN
	ESCC úroveň B	ESCC úroveň C	DSCC
	JAXA QTS třída I	JAXA QTS třída II	
Pasivní součástky	MIL třída S,T	MIL "P" failure rate	MIL "M" a "L" intenzita poruch
	MIL "S" intenzita poruch	MIL Weibull "B"	DSCC
	MIL "R", pokud není "S" QPL	ESCC úroveň C	
	MIL Weibull "C" ("D" pokud je k dispozici)	JAXA QTS třída II	
	ECSS úroveň B		
	JAXA QTS třída I		

Označení úrovně kvality:

- MIL - vojenský standard
- ESCC - Evropská spolupráce pro standardizaci v oblasti kosmických aktivit
- DSCC - Americký vojenský standard kvality (Defense Supply Center Columbus)
- JAXA - Japonská národní vesmírná agentura

Dále intenzitu poruch ovlivňuje i pracovní prostředí. Zařízení budou odlišně zatěžována na zemi, ve vzduchu nebo právě ve vesmíru. Součinitel prostředí se označuje π_E . Pro vesmírná zařízení se předpokládá prostředí S_F (Space, Flight). Odhady spolehlivosti byly vždy přesnější pro zemské prostředí, jelikož zde většina zkoušek a testů probíhala. Pro vesmírné využití je často nutné se spolehnout na simulaci vesmírného prostředí, což může přidávat další nepřesnosti. [31]

Mezi nedostatky predikce intenzit poruch patří odhady poruchovosti získané z naměřených dat. Ty jsou platné pouze pro podmínky, při kterých byly získány. Určitá interpolace dat je možná, ale vzhledem k použití empirických modelů je značně omezená. Dokonce i v případě podobných podmínek použití zařízení se mohou výsledky predikce intenzit poruch výrazně lišit. [31]

Pro výpočet intenzity poruch lze využít i další možnosti: [11]

- Databáze výrobců a uživatelů – jedná se především o údaje ze zkoušek na konkrétních součástkách, interních testování nebo odborných úsudků
- Příručky bezporuchovosti – příruček pro výpočet bezporuchovosti je několik, patří mezi ně právě MIL-HDBK-217, mezi další používané patří: FIDES, PRISM, RDF 2000 aj.

3.3.2 Blokové diagramy bezporuchovosti (RBD)

Blokové diagramy bezporuchovosti nám vizuální formou ukazují logické vztahy a propojení mezi všemi prvky v systému. To přináší možnost přehledné identifikace poruchových cest a samotných poruch. Nutno mít na paměti, že blokové diagramy bezporuchovosti neodpovídají blokovým diagramům funkčního uspořádání systému. Samotná analýza spočívá v rozložení a zjednodušení celého blokového diagramu bezporuchovosti na jednodušší bloky, které je možné samostatně analyzovat. Nutným požadavkem na provedení analýzy je dostatečné porozumění funkce analyzovaného systému a jeho konceptu zálohování. [32,34]

Pro zachování dostatečné přehlednosti je každý blokový diagram bezporuchovosti označován názvem včetně některých podrobnějších informací ohledně mise. Dále by měl každý blokový diagram bezporuchovosti obsahovat výpis veškerých podmínek a omezení, které ovlivňují výběr provedení diagramu, spolehlivostní parametry a souhrn platných zjednodušení a omezení pro vývoj diagramu. [32]

Bloky v diagramu jsou logicky uspořádány vzhledem k posloupnosti událostí předepsaného provozu. Všechny funkční prvky a události v blokovém diagramu musí být jednoznačně identifikovatelné. Jednotlivé bloky zastupují funkční prvky a mohou být zapojeny. [32]

- Sériově

Jedná se o nejjednodušší strukturu zapojení prvků. V případě selhání pouze jednoho prvku v sériové struktuře dojde k poruše celého objektu. Systém se ve stavu bezporuchovosti nachází pouze v případě, že jsou bezporuchovém stavu všechny prvky. Často se princip sériového zapojení používá pro určení odhadu bezporuchovosti celého systému v počátečních fázích návrhu nebo pro zjištění prvotního odhadu u složitějších struktur systému. V případě využití principů sériového systému pro složitější strukturu se počítá s nejhorším případem, a tedy nejnižší pravděpodobností bezporuchového stavu. Přílišné zjednodušení modelu může vést ke zbytečnému zvyšování robustnosti systému, jehož následkem může být extrémní nárůst hmotnosti a ceny. Z toho důvodu je nutné volit zjednodušení modelu s opatrností. [21]



Obr. 6 Sériová struktura zapojení bloků

Výpočet pravděpodobnosti bezporuchovosti sériové struktury zapojení:

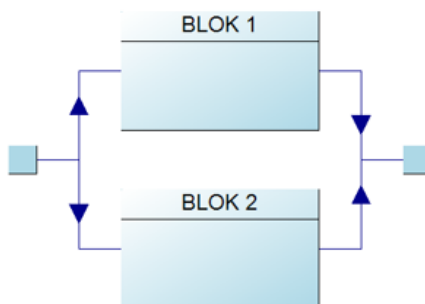
$$P_{sér.} = P_1 P_2 \dots P_n = \prod_{i=1}^n P_i \quad (3.12)$$

kde pro výpočet bezporuchovosti i-tého prvku platí vztah:

$$P_i = \exp(-\lambda_i t) \quad (3.13)$$

- Paralelně

Ve své podstatě se jedná o pravý opak sériového zapojení. K poruše celého objektu tak dochází až v případě selhání všech jeho prvků. Systém je ve stavu bezporuchovosti, pokud alespoň je v bezporuchovém stavu alespoň jeden prvek. V případě využití dané struktury zapojení se počítá s nejvyšší pravděpodobností bezporuchového stavu. Často se paralelní struktura zapojení využívá pro zálohování prvků kvůli vyšší pravděpodobnosti bezporuchovosti. [21]



Obr. 7 Paralelní struktura zapojení bloků

Výpočet pravděpodobnosti bezporuchovosti paralelní struktury zapojení s prvky A a B:

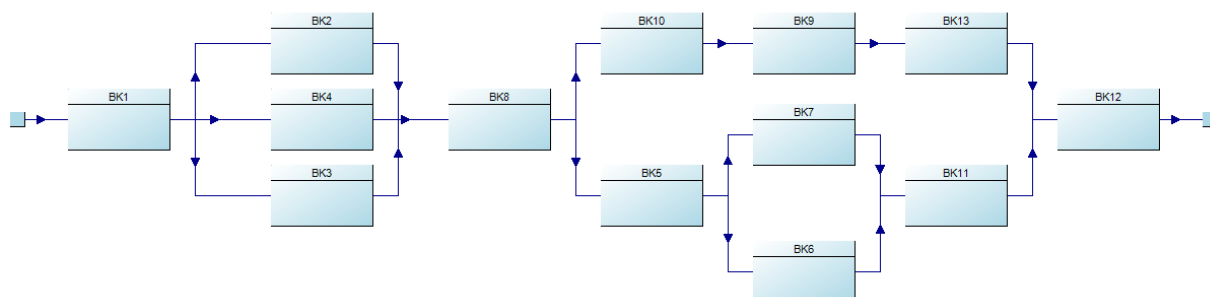
$$P_{par.} = 1 - \prod_{i=1}^n (1 - P_i) \quad (3.14)$$

kde pro výpočet bezporuchovosti i-tého prvku platí vztah:

$$P_i = \exp(-\lambda_i t) \quad (3.15)$$

- Kombinovaně (sériově i paralelně)

V praxi se nejčastěji setkáváme se strukturou zapojení současně sériovou i paralelní, tedy kombinovanou. Pro výpočet daného zapojení se většinou využívá metoda dekompozice nebo inspekční metoda, pomocí kterých se se složité systémy výrazně zjednodušují. [21]



Obr. 8 Kombinovaná struktura zapojení bloků

Obecné předpoklady pro blokové diagramy bezporuchovosti: [32]

- Jednotlivé bloky zastupují elementy nebo funkční prvky.
- Spojovací čáry slouží pouze jako spojovací prvky mezi bloky a nemají žádnou hodnotu bezporuchovosti.
- Všechny vstupy prvků jsou v rámci specifikačních limitů
- Porucha jednoho elementu (bloku) způsobuje poruchu celého prvku, pokud zde není jiná alternativní nebo záložní možnost.
- Každý element (blok) v diagramu je nezávislý vůči ostatním elementům s ohledem na pravděpodobnost poruchy.

3.4 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)

FMECA je jednou z metod zajištění spolehlivosti, která zkoumá a charakterizuje možné způsoby selhání a stanovuje jejich případný vliv na celý systém, ale i podsystémy a další vybavení. Každý možný způsob poruchy je hodnocen podle jeho dopadu na úspěšnost mise, bezpečnost osob a vybavení. FMECA je složena z těchto dvou analýz: [35]

- FMEA (Analýza způsobu a důsledků poruch)
- CA (Analýza kritičnosti).

Metoda FMEA byla původně vyvinuta agenturou NASA, aby zlepšila a ověřila bezpečnost vesmírných programů. Vývoj metody měl sloužit především pro organizované a systematické analyzování způsobů poruch systému a následných důsledků na jednotlivé podsystémy i samotný systém. Důvodem vývoje metody bylo zlepšení zabezpečení spolehlivosti a bezpečnosti u novějších a složitějších systémů, kdy v případě nedostatečného zabezpečení hrozily katastrofické nebo kritické důsledky. Vůbec poprvé byla daná metoda použita u kosmického projektu Apollo. [21,32]

FMEA jako samostatná analýza je možná a běžně se používá, avšak analýzu kritičnosti bez předchozího zpracování FMEA nelze provést, jelikož je třeba nejprve určit kritické způsoby poruch. [32]

FMEA je vhodná kromě oblasti spolehlivosti i pro hodnocení bezpečnosti. Konkrétně standardy ECSS-Q-ST-30C a ECSS-Q-ST-40C rozlišují důsledky selhání na spolehlivostní a bezpečnostní. Ve spolehlivosti je brán ohled především na funkci systému pro správné splnění mise. Bezpečnost se zabývá také ochranou lidského zdraví, okolních zařízení a životního prostředí. Důsledky selhání dle spolehlivosti a bezpečnosti jsou znázorněny v Tab. 12. Konkrétní zařazení důsledků selhání do příslušných bezpečnostních kategorií je na dohodě zákazníka a dodavatele zařízení. [10]

V případě, že mezi zákazníkem a dodavatelem neexistuje dohoda o hodnocení závažnosti na úrovni nižší než systémové, dovoluje standard ECSS-Q-ST-30-02C přiřadit hodnocení závažnosti důsledků selhání tak, že ztrátou mise se rozumí ztráta primární funkce zařízení. [10]

Tab. 12 Hodnocení závažnosti důsledků na systémové úrovni nebo úrovni satelitu [10]

Kategorie závažnosti	Úroveň závažnosti	Důsledky selhání	
		Spolehlivost	Bezpečnost
Katastrofická	1	Šíření poruchy (pro analýzy na nižší než úrovni satelitu)	Ztráta života
			Ztráta řídicího rozhraní systému s lidskou posádkou
			Ztráta vybavení kosmodromu
			Kritické důsledky pro životní prostředí
			Ztráta systému
Kritická	2	Ztráta mise	Dočasné zranění neohrožující život
			Závažné důsledky pro životní prostředí
			Závažné poškození řídicího rozhraní systému
			Závažné poškození pozemních zařízení
Závažné	3	Větší degradace mise	
Nezávažné	4	Menší degradace mise	

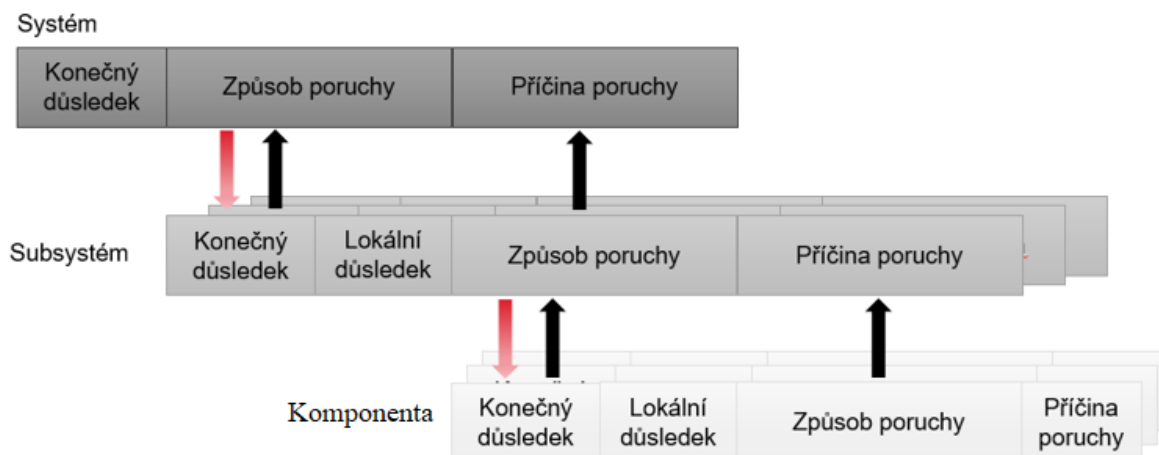
Hodnocení závažnosti důsledků se provádí bez ohledu na možné způsoby kompenzace poruchy a nezohledňují se redundantní řešení jako v letectví. Pro vesmírné prostředky je to řešeno tak, že se za hodnocení úrovně závažnosti přidávají přípony: [10,35]

- SP (Single Point Failure) – selhání položky může mít za následek selhání celého systému a není nijak kompenzováno
- R (Redundancy) – selhání položky může mít za následek selhání celého systému pouze v případě selhání i ostatních položek plnících stejnou funkci (zálohování)
- SH (Safety Hazard) – selhání položky může mít následky také v oblasti bezpečnosti, využívá se především u zařízení s lidskou posádkou

Předpokládá se, že identifikovaný způsob poruchy je jedinou poruchou systému nebo vybavení. Kombinace více poruch se nepředpokládá. V oblasti prediktivních analýz patří FMEA k nejpoužívanějším metodám, a to nejen v technických oblastech. [21]

FMEA je ve své podstatě strukturovaná analýza postupující zdola nahoru (bottom-up), která zvláště zvažuje každý elementární režim selhání a snaží se odhadnout a stanovit jeho důsledky. Analýza zpravidla začíná na nejnižší úrovni systému (součástky) a hierarchicky postupuje směrem k dalším úrovním, subsystémům, a nakonec i systému samotnému a zkoumá možné poruchy, které mohou mít vliv na celý systém. Postup je opačný než u FTA (analýza stromu poruchových stavů), u které se začíná poruchou hlavního systému a hierarchicky směrem dolů se hledají příčiny (causes) způsobující selhání právě hlavního systému. Na Obr. 9 je znázorněn hierarchický postup analýzy FMEA. Černé šipky znázorňují posun analýzy na vyšší úroveň. Způsob poruchy některé součástky na nižší úrovni může zapříčinit poruchu na vyšší úrovni.

Stejně tak konečný důsledek poruchy součástky se může stát způsobem poruchy vyšší úrovně. Červené šipky směrem dolů reprezentují rozpad požadavků z vyšší úrovně na nižší úroveň. [10,21,32]



Obr. 9 Hierarchický postup FMECA analýzy [10]

FMEA je efektivní metoda při rozhodování během procesu vývoje. Důležitým předpokladem je včasná a opakovaná implementace v různých fázích vývoje produktu. V případě pozdního využití metody dochází ke značnému omezení možností využití nástroje pro zlepšení návrhu a vývojových procesů, případně k významným finančním ztrátám v důsledku nevyhnutelného přepracování návrhu. [10]

FMEA poskytuje: [32,35]

- možnost volby návrhu s vysokou pravděpodobností úspěchu mise a bezpečnosti posádky
- zdokumentovaný seznam prvků systému, jejich režimy selhání a vliv na úspěšnost mise
- základ pro včasné odhalení případných problémů v systému a jejich zamezení
- seznam poruch, závažnost a pravděpodobnost jejich výskytu
- identifikování kritických prvků a poruch, které mohou vést k narušení či selhání mise
- brzké vstupní informace pro plánování testovacích zkoušek
- vstupní hodnoty pro další analýzy a odhady
- nástroj, který slouží k hodnocení návrhu

FMEA odhaluje potenciální problémy se spolehlivostí zařízení, které musí být nutně eliminovány nebo alespoň minimalizovány pomocí modifikací návrhu. Mezi poruchy, které je možné identifikovat patří: [35]

- poruchy některého obvodu, které se mohou šířit a vést k poruchám kritického obvodu.
- oblasti, kde jsou požadovány fail-safe, fail-soft nebo fail-operational koncepty.
- primární poruchy, které mohou způsobovat další sekundární poruchy (tzv. kaskádovité poruchy).

Dalším konceptem, který rozšiřuje původní rozsah metody FMEA je tzv. šíření (propagace) poruchy. Šíření poruchy je definováno jako fyzická nebo logická událost, která je způsobena selháním produktu a může dále vyústit v selhání produktů, které nespádají do analyzované oblasti (poškození externího produktu nebo systému). Mimo identifikování kritických míst návrhů pomáhá nalézt implementační chyby návrhu, které by mohly způsobit porušení

definované strategie zálohování. Zdroje propagace poruchy jsou nejčastěji: elektrické rozhraní, termální rozhraní, rozhraní software-hardware. [30]

Ideální a vhodné je, pokud je analýza naplánovaná a dokončovaná současně s celým navrhovacím procesem a stává se tak jeho součástí. Je tedy zapojena v prvotních fázích návrhu až po návrh finální, který by měl zahrnovat výsledky a další doporučení. V případě jakékoliv úpravy a změny v návrhu je nutno poupravit i samotnou analýzu. [10,35]

Analýza kritičnosti (CA) přidává do FMEA kvantitativní hodnocení kritičnosti na základě hodnocení závažnosti důsledků (SN) a pravděpodobnosti jejich nastoupení (PN). Tímto postupem je možné stanovit kritické součásti a provést nápravné akce. Podle ECSS-Q-ST-30-02C je stanovení hodnocení kritičnosti následující: [10]

$$CN = SN \cdot PN \quad (3.16)$$

Převod hodnocení závažnosti důsledku na faktor závažnosti SN je znázorněn v Tab. 13.

Tab. 13 Faktor závažnosti, kategorie závažnosti a úroveň závažnosti [10]

Faktor závažnosti SN	Kategorie závažnosti	Úroveň závažnosti
4	Katastrofická (Catastrophic)	1
3	Kritická (Critical)	2
2	Závažná (Major)	3
1	Nezávažná (Negligible)	4

Druhé významné číslo ovlivňující faktor kritičnosti (CN) je faktor pravděpodobnosti (PN). Určuje se z Tab. 14 na základě pravděpodobnosti výskytu poruchy. Tabulka pravděpodobnosti výskytu poruchy může být libovolně upravena podle potřeb zákazníka. [10]

Tab. 14 Pravděpodobnost výskytu poruchy a faktor pravděpodobnosti [10]

Pravděpodobnost výskytu poruchy		Faktor pravděpodobnosti PN
Pravděpodobný (Probable)	$P > 1.10^{-1}$	1
Příležitostný (Occasional)	$1.10^{-3} > P \geq 1.10^{-1}$	2
Nepravděpodobný (Remote)	$1.10^{-5} > P \geq 1.10^{-3}$	3
Extrémně nepravděpodobný (Extreme remote)	$P \leq 1.10^{-5}$	4

Konečně se ze získaných faktorů závažnosti a pravděpodobnosti určuje, zda prvek spadá mezi kritické prvky. Kritický prvek je takový, který: [10]

- má hodnocení v matici kritičnosti 6 nebo více
- spadá do katastrofické kategorie závažnosti (faktor závažnosti SN=4)

Tab. 15 Matice kritičnosti [10]

Kategorie závažnosti	SN	Pravděpodobnost nastoupení			
		10^{-5}	10^{-3}	10^{-1}	1
		PN			
		1	2	3	4
Katastrofická	4	4	8	12	16
Kritická	3	3	6	9	12
Závažná	2	2	4	6	8
Nezávažná	1	1	2	3	4

Výsledná analýza nás s důrazem informuje o možných poruchách, které mohou ohrožovat dokončení mise. Hodnotí závažnosti jednotlivých poruch v konečném důsledku na úspěšnost podstupované mise. Poskytuje odhad o závažnosti kritických poruch a kvantitativně hodnotí režimy selhání celého systému i jeho subsystémů. A také nám napomáhá v odhalení kritických součástí z hlediska bezpečnosti a spolehlivosti. [35]

4 Bezpečnost vesmírných prostředků

Program zajištění bezpečnosti má za úkol předcházet nehodám a kontrolovat veškerá nebezpečí spojená s návrhem, výrobou, transportem a provozem vesmírného produktu. Pro mise s lidskou posádkou je program bezpečnosti jasně zaměřený především na bezpečí a ochranu zdraví osob během celé mise. U misí bez posádky se tento záměr ubírá především k ochraně zařízení, ale i zde se na základě zkušeností z minulosti nesmí podceňovat bezpečnost pracujících osob. Do této oblasti spadá práce s nebezpečnými látkami, vysokonapěťovými zdroji, ale třeba i běžné logistické úkoly a skladování. Cílem je zajistit, aby všechna rizika byla adekvátní vzhledem k důsledkům, identifikována, minimalizována, kontrolována a přijata prostřednictvím programu zajištění bezpečnosti. [14,20]

Bezpečnostní standard ECSS-Q-ST-40C se zabývá: [14]

- Eliminací hrozícího nebezpečí pro:
 - Lidské životy
 - Životní prostředí
 - Veřejný i soukromý majetek
 - Kosmickou loď a nosnou raketu
 - Podpůrné pozemní vybavení
- Určováním a vyhodnocováním bezpečnostních rizik spojených s aktivitami vesmírného projektu
- Technicky a nákladově efektivním způsobem minimalizací bezpečnostních rizik
- Zajištěním dostatečného ověření bezpečnostních kontrolních opatření

Tab. 16 Kategorie závažnosti nebezpečí [14]

Dopad na: ↓	Kategorie závažnosti nebezpečí		
	Katastrofické	Kritické	Závažné a nezávažné
Lidské životy	Ztráta života, život ohrožující zranění nebo zranění s trvalými následky	Zranění s dočasnými následky bez ohrožení života	----
Pozemní vybavení	Ztráta pozemního vybavení	Závažné poškození pozemního vybavení	----
Kosmická loď s nosnou raketou	Ztráta zařízení	Závažné poškození	----
Veřejný i soukromý majetek	---	Ztráta nebo závažné poškození majetku	----
Životní prostředí	Závažné škodlivé účinky na životní prostředí	Krátkodobé škodlivé účinky na životní prostředí	---

Tabulka závažností nebezpečí není pevně stanovená a může se odlišovat na základě požadavků zákazníka. [14]

Program bezpečnosti zajišťuje, že: [14]

- Bezpečnost je navržena do systému
- Bezpečnostní kontroly jsou v plánu ověření náležitě verifikovány
- Bezpečnostní požadavky kosmodromu jsou splněny
- Všechna nebezpečí jsou eliminována, případně minimalizována tam, kde úplná eliminace není možná

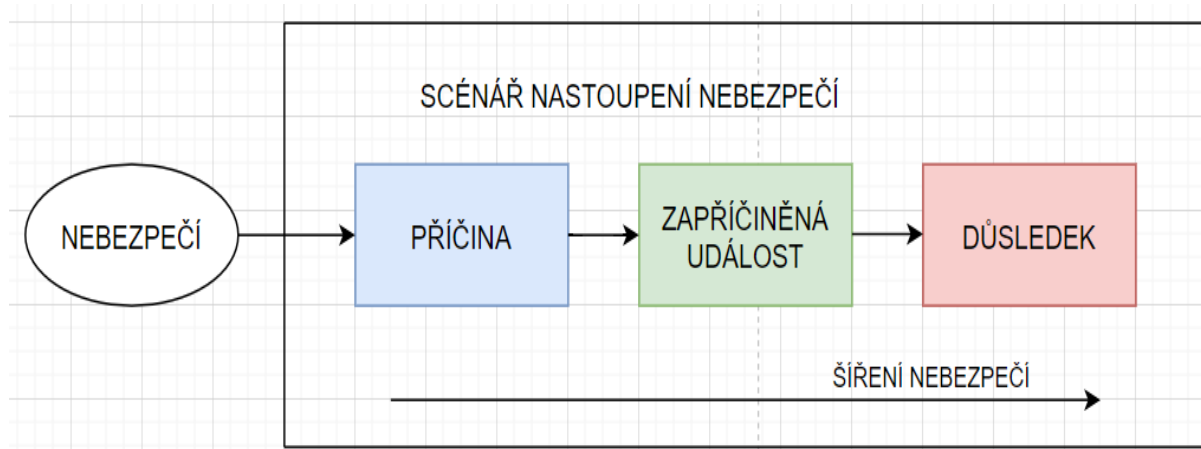
Program bezpečnosti se skládá z: [14]

- Identifikace a kontroly všech rizik s ohledem na návrh, vývoj a provoz vesmírných produktů
- Posouzení rizik na základě kvalitativních a kvantitativních analýz
- Uplatnění priority snižování nebezpečí a kontrolních opatření na zbývajících rizika

4.1 Analýza nebezpečí (Hazard Analysis)

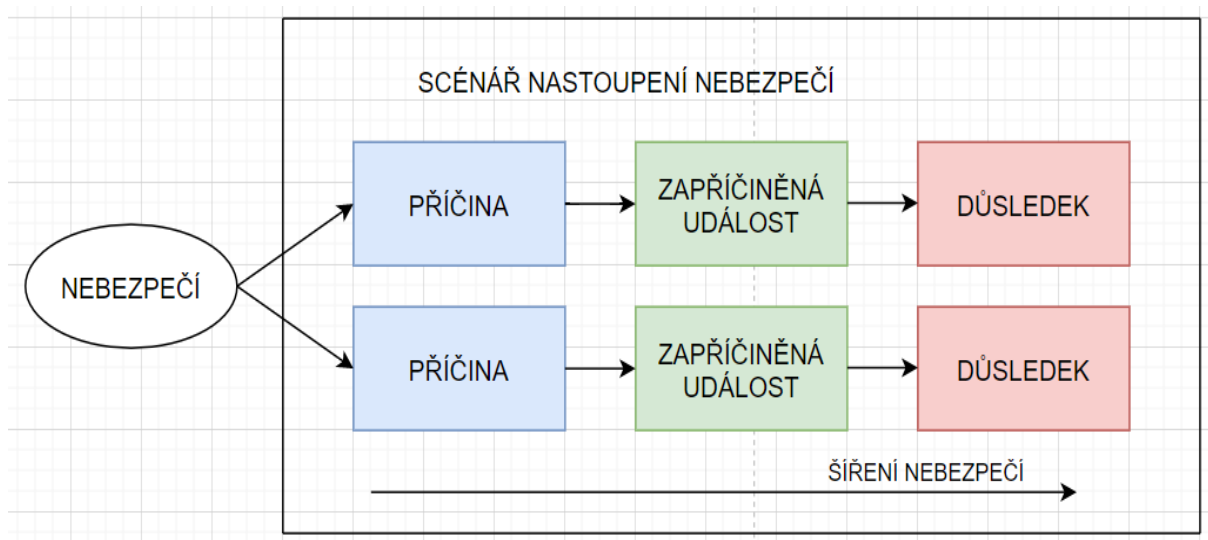
Analýza nebezpečí je metoda založena na hledání, hodnocení a snižování nebezpečí a rizik během všech fází vesmírného projektu. Zkoumá potenciální i existující nebezpečí, která mohou vyústit v nehodu. Analýzu nebezpečí je možné propojit i s ostatními metodami určenými k zajištění bezpečnosti a spolehlivosti, zejména FMECA. [13]

Nebezpečí je podmíněno nastoupením scénáře nebezpečí. Z počáteční příčiny vznikne zapříčiněná událost, která vyúští v konečný důsledek. Ten je spojen s pozorovatelnými příznaky v systému. Důsledky pro bezpečnost jsou charakterizovány podle jejich závažnosti. [13]

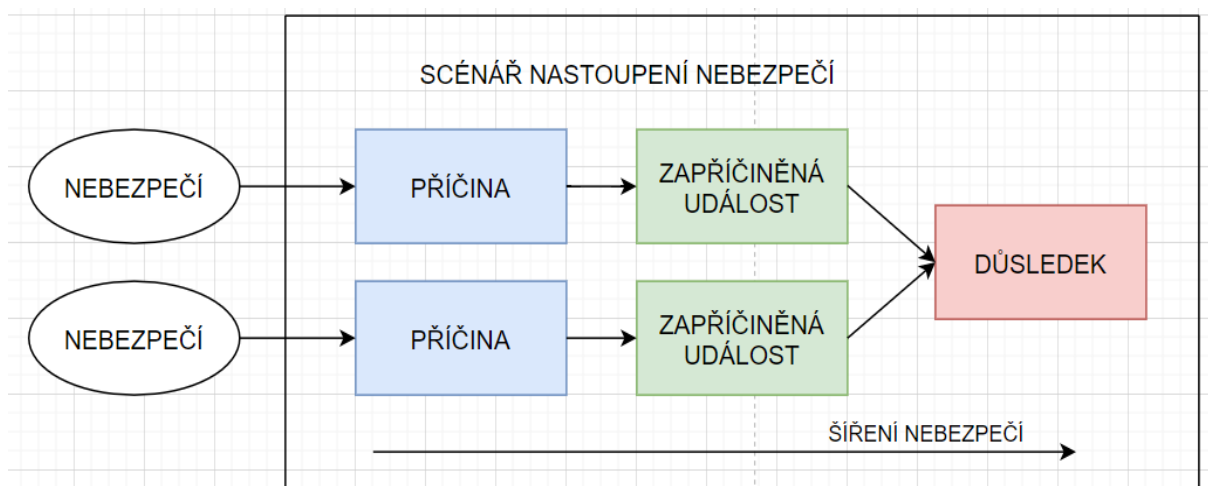


Obr. 10 Nebezpečí a scénář nastoupení jeho nastoupení [13]

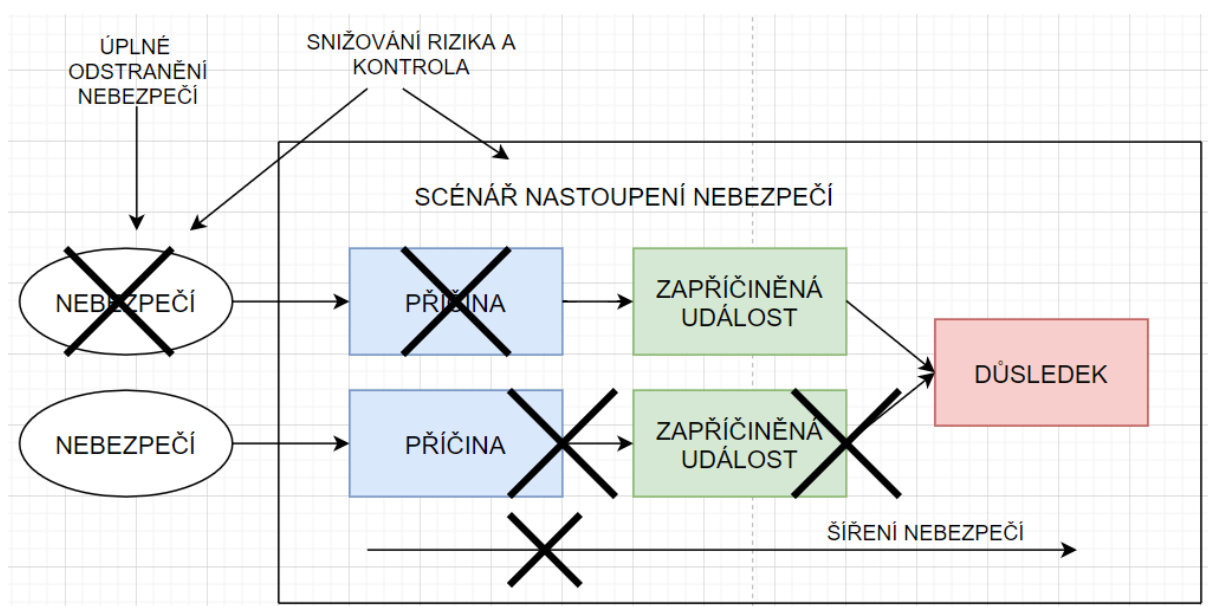
Obr. 10 znázorňuje nejjednodušší schéma šíření nebezpečí od příčiny až po důsledek. Ve skutečnosti se však může vyskytovat větší množství kombinací příčin a díky nim vzniklých událostí, důsledků i nebezpečí jako takových. Jedno konkrétního nebezpečí může být způsobeno více příčinami a vést na několik možných scénářů viz. Obr. 11. A také vícero nebezpečí může vést ke stejnému konečnému důsledku viz. Obr. 12. [13]



Obr. 11 Nebezpečí a scénář jeho nastoupení (Vznik více scénářů z jednoho nebezpečí) [13]



Obr. 12 Nebezpečí a scénář jeho nastoupení (Vznik jednoho důsledku z více nebezpečí) [13]



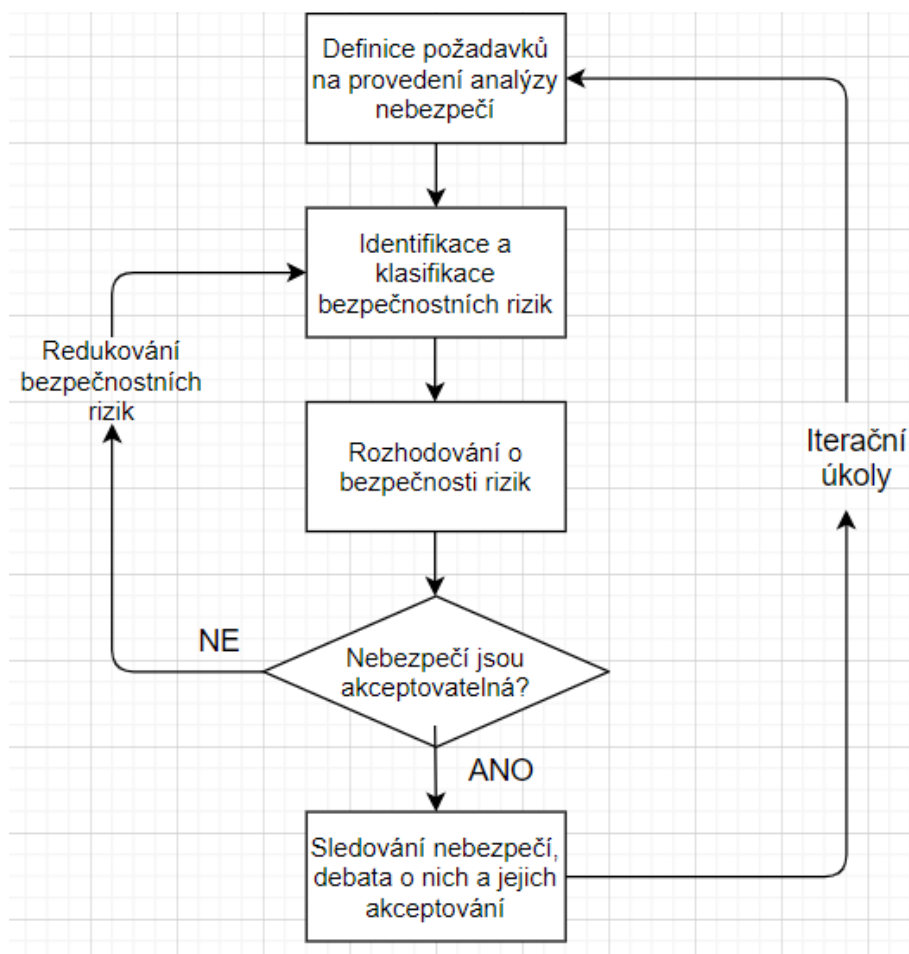
Obr. 13 Možnosti eliminování a snižování nebezpečí [13]

Snahou je se maximálně vyvarovat nastoupení nebezpečné události. Nejčastěji úplnou eliminací odstraněním potenciálně nebezpečných vlastností systému. V případě nemožné eliminace se daná nebezpečí alespoň minimalizují a kontrolují. Minimalizací se rozumí snižování množství nebo úrovně rizik potenciálně nebezpečných prvků. Kontrola je prováděna preventivními opatřeními nebo snižováním pravděpodobnosti výskytu a zmírněním výsledných důsledků. Podle průvodních příznaků je možno detekovat některé vznikající události, které mohou vést k nebezpečné události a včas je zamezit. Možnosti eliminování a snižování nebezpečí jsou znázorněny na Obr. 13. [13]

Analýza nebezpečí je hlavní bezpečnostní analýza, která napomáhá inženýrům a lidem v oboru začlenit aspekty bezpečnosti do technických postupů a rozhodovacích procesů ve všech fázích vesmírného projektu. Poskytuje základní vstup pro hodnocení bezpečnostních rizik systému. Proces analýzy nebezpečí je složen z několika postupných kroků, které jsou nutné pro eliminování a snižování bezpečnostních rizik. Základní postup je následující: [13]

- Definice požadavků na provedení analýzy nebezpečí
- Identifikace a klasifikace bezpečnostních rizik
- Rozhodování o bezpečnosti rizik
- Sledování rizik, debata o nich a jejich akceptování

Jedná se o iterační proces, kdy se hledá vhodné a akceptovatelné řešení. V případě, že nebezpečí nejsou akceptovatelná, je nutné je minimalizovat a opět opakovat některé kroky. [13]



Obr. 14 Postupný proces analýzy nebezpečí [13]

Analýza využívá iteračních operací, jejichž množství záleží na obtížnosti analyzovaného systému. Obtížnost je určena dle požadavků na analýzu, její typ a průběžnou fázi. Často se jedná o týmovou práci a je nutná odpovědnost všech zúčastněných osob zabývajících se konkrétními úkoly během celé analýzy. Výsledný produkt analýzy je využíván jako vstup během vývoje systému. Je požadováno, aby byl průběh analýzy vždy v souladu s postupovými kroky a úkoly a dokumentace dosažených výsledků odpovídala příslušné standardizaci viz Tab. 17. [13]

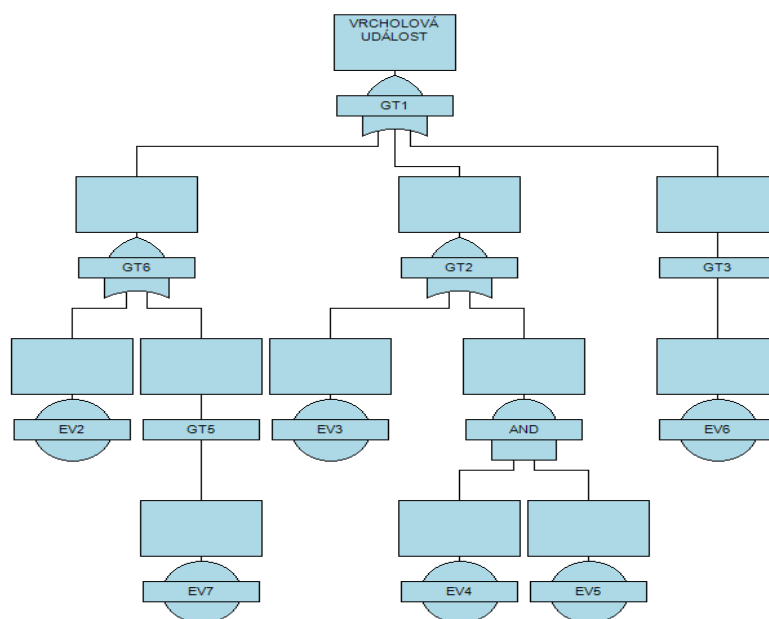
Tab. 17 Úkoly obsažené v postupných krocích analýzy nebezpečí [13]

Krok	Popis kroku	Úkol	Popis úkolu
1	Definice požadavků na provedení analýzy nebezpečí	1	Definování rozsahu, cílů a plánování analýzy nebezpečí
		2	Definování systému, který bude analyzován
2	Identifikace a klasifikace bezpečnostních rizik	3	Identifikování projevu nebezpečí
		4	Identifikování a klasifikování scénářů nastoupení nebezpečí
3	Rozhodování o bezpečnosti rizik	5	Rozhodování o akceptování nebezpečí
		6	Redukování nebezpečí
		7	Schvalování přijetí nebezpečí
4	Sledování nebezpečí, debata o nich	8	Sledování a řešení nebezpečí
		9	Akceptování nebezpečí

4.2 Analýza stromu poruchových stavů (FTA)

Prvotní vývoj a použití analýzy stromu poruchových stavů proběhl během vývoje startovacího systému rakety Minuteman. Další vylepšení přišlo díky firmě Boeing využitím výpočetní techniky. Postupem času analýza našla uplatnění ve většině technických oborů a v současnosti patří mezi nejpoužívanější metody bezpečnosti a spolehlivosti. [21]

FTA je deduktivní metoda, která znázorňuje pomocí logického grafu vztahy mezi vrcholovou událostí a jejími příčinami. Během analýzy se postupuje od vrcholové události k událostem na nižších úrovních. Hledají se právě takové události a jejich kombinace, které vedou ke vzniku vrcholové události. V případě, že je analýza zpracována důsledně a jsou v ní zobrazeny veškeré možné příčiny poruch, tak lze velmi dobře odhalit nejslabší místa systému v počátečních fázích projektu. Množství možných kombinací je znázorněno pomocí větvení stromu. Čím je systém složitější a obsahuje více prvků, tím je zpravidla větší i strom poruchových stavů. Zpracování analýzy stromu poruchových stavů složitějšího systému s velkým počtem prvků a velkým množstvím poruchových kombinací je velmi obtížné a časově náročné. V praxi se k omezení větvení stromu poruchového stavu s úspěchem využívá metody FMECA. Možnosti provedení analýzy jsou: kvalitativní, kvantitativní nebo kombinované. Výsledný výstup podává informace o veškerých potenciálních poruchových místech v systému, pravděpodobnosti vzniku poruchy a výsledné poruchovosti celého systému v časovém intervalu. Jako u ostatních zmíněných analýz je vyžadována důkladná znalost analyzovaného systému. [21,34]



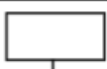
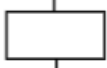





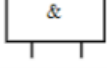

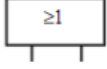

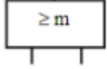
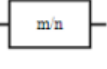

Obr. 15 Vzorový strom poruchových stavů

Jak již bylo zmíněno, u analýzy stromu poruchových stavů se postupuje opačným směrem než u FMECA, tudíž shora dolů. Z toho důvodu je zde větší pravděpodobnost nepřesností a chyb na nejnižších úrovních systému. Význam analýzy je především u zařízení se složitějšími kombinacemi možných poruch, kdy právě kombinace některých nekritických událostí může vyvrcholit v nežádoucí kritickou událost. Nejčastěji se analýza využívá pro funkční větve a rozhraní, jejichž poruchy mohou mít kritický dopad na bezpečnost mise a personálu. Výsledná analýza poskytuje názorný přehled možných kombinací, které mohou vést k předem stanovené kritické události. Kvalita výsledků analýzy se odvíjí především od správnosti zpracování nebo zvolené úrovně, vhodně použitých vstupních dat a jejich přesnosti. Aplikace metody je možná

již v počátečních návrhových fázích (pro generování požadavků na nižší úrovni) a postupně ji lze vylepšovat během celého procesu vývoje. Chyby a nepřesnosti na počátku mohou mít výrazný vliv na výsledek celé analýzy. [32]

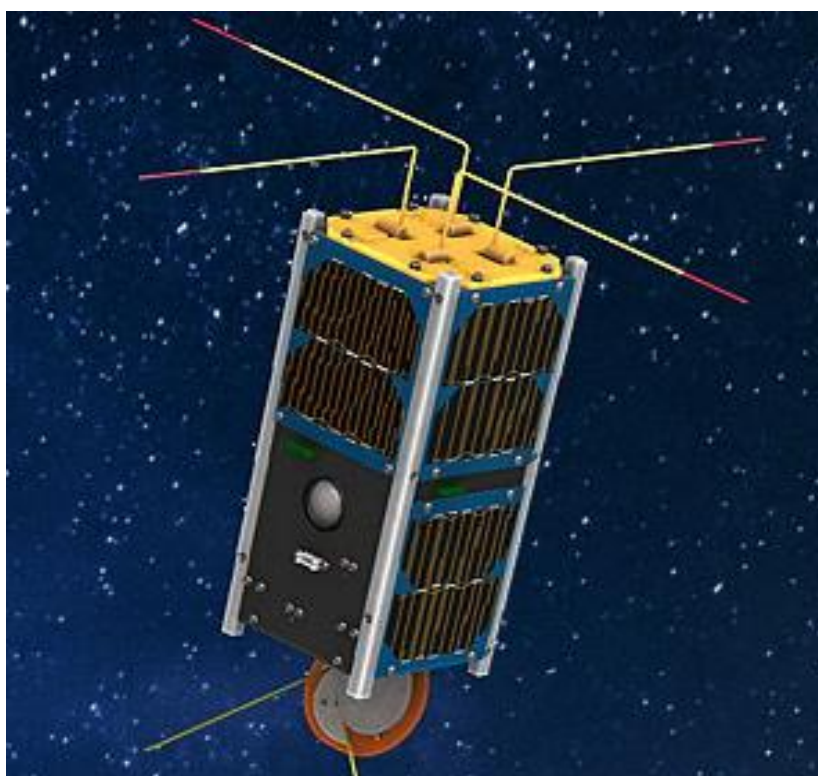
V logickém grafu analýzy stromu poruchových stavů se využívá obrázkových symbolů. Jednotlivé symboly představují logické vztahy mezi prvky ve stromu. Příklad těch nejčastěji používaných i s vysvětlením je znázorněn v Tab. 18.

Tab. 18 Schématické značky používané pro sestavení stromu poruch [21]

Doporučená značka	Alternativní značka	Název a popis
		Blok s názvem nebo popisem vrcholové události (TOP jevu).
		Blok s názvem nebo popisem události (jevu), případně s uvedením pravděpodobnosti výskytu (pokud se to požaduje).
		Základní (primární) událost – událost, která se dále nedělí.
		Nerozvíjená událost – událost, která není dále rozvíjená (zpravidla proto, že se to nepovažuje za nutné)
		Událost analyzovaná jinde – událost dále rozvíjená v jiném stromu poruch.
		Přenos do – událost definovaná kdekoli jinde ve stromu poruch.
		Přenos ven – opakovaná událost použitá kdekoli jinde ve stromu poruch.
		Hradlo AND (a) – událost nastane pouze tehdy, když současně nastanou všechny vstupní události.
		Hradlo OR (nebo) – událost nastane tehdy, když nastane kterákoliv vstupní událost, nebo jejich libovolná kombinace.
		Zálohovaná struktura – událost nastane tehdy, jestliže nastane minimálně m z n vstupních událostí.
		Hradlo INHIBIT (zdržení) – událost nastane pouze tehdy, když nastane vstupní událost a současně je splněna podmínka vyznačená uvnitř značky.

5 Satelit UPSat

Satelit, na kterém budou aplikovány bezpečnostní a spolehlivostní metody. UPSat patří do rodiny satelitů tzv. kostkového typu (CubeSat). Základní rozměr kostkového stavebního bloku je 10 x 10 x 10 cm, při maximální hmotnosti 1,33 kg. Postupem času se z důvodů zvyšování požadavků začaly dané stavební bloky modulárně skládat. Jeden stavební blok o základních rozměrech odpovídá hodnotě 1U. [27] Satelit UPSat je složen ze dvou stavebních bloků a označuje se tedy jako 2U. Na jeho výrobě a vývoji se podílela Univerzita Patras a Libre Space Foundation. Cílem mise satelitu UPSat bylo vytvoření a následné vyslání na oběžnou dráhu prvního satelitu s open source hardwarem a softwarem. K úspěšnému vypuštění rakety Atlas-V, která daný satelit vynesla k ISS došlo v dubnu roku 2017. O měsíc později byl z ISS satelit vypuštěn na oběžnou dráhu. Mise satelitu UPSat trvala přibližně 18 měsíců. [26]

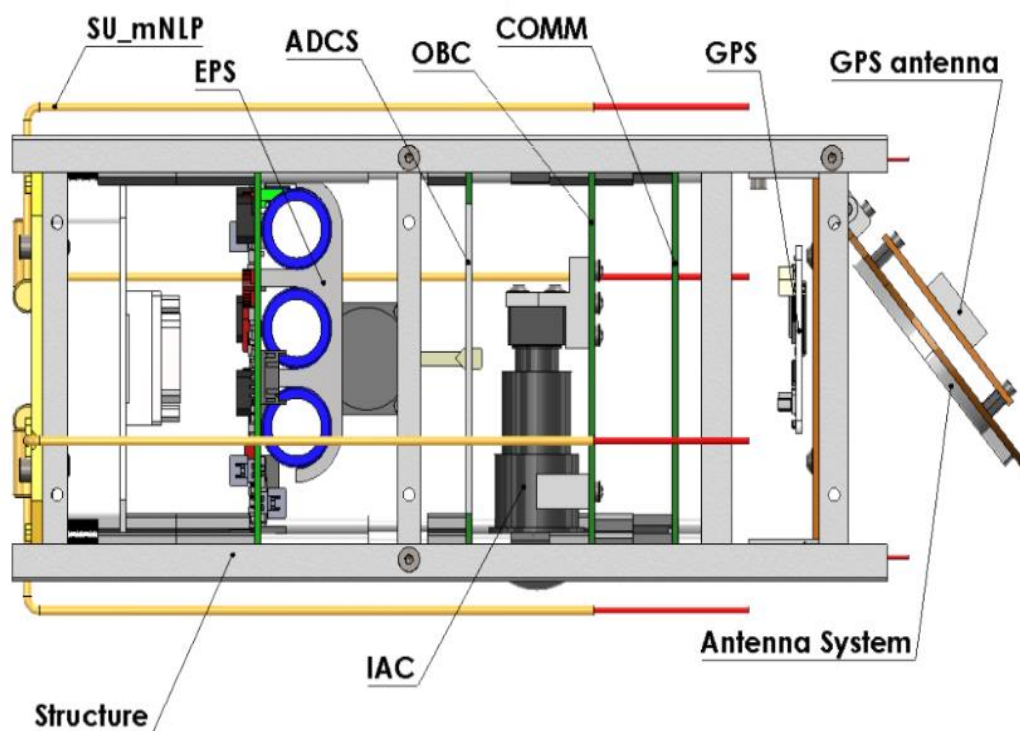


Obr. 16 Satelit UPSat [24]

5.1 Rozdělení satelitu UPSat

Satelit UPSat lze rozdělit na:

- Nosná konstrukce satelitu
- EPS-elektrický zdrojový systém
- IAC-systém pro získávání obrazu
- SU-vědecká jednotka
- ADCS-systém určování polohy a řízení satelitu
- OBC-Palubní počítačový systém
- COMMS-Komunikační systém [26]



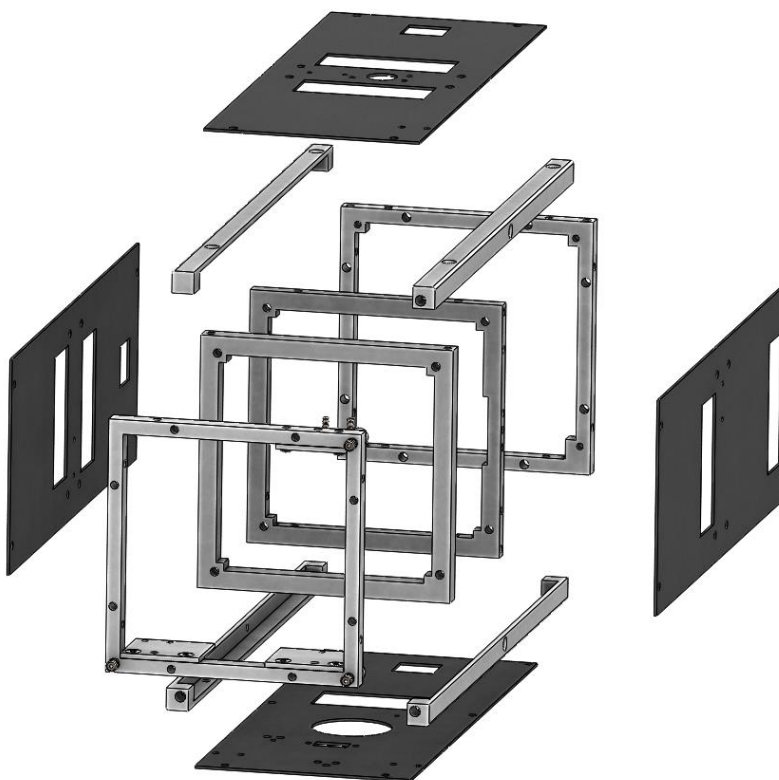
Obr. 17 Systémy satelitu UPSat [26]

5.1.1 Nosná konstrukce satelitu

V rámci nosné konstrukce satelitu UPSat je využito hybridního použití kompozitních materiálů a hliníkových slitin. Vzhled a tvar má konstrukce základ v komerčně dostupných satelitech CubeSat. Z důvodu velmi dobrých mechanických vlastností a úspory hmotnosti je rám složen ze 4 hliníkových kolejnic a 4 hliníkových čtvercových přepážek, ke kterým jsou uchyceny desky elektronických obvodů. Dále jsou použity 4 kompozitní stěny, u kterých bylo cílem dosáhnout nejlepší laminace, aby odolaly aplikovanému zatížení a napomáhali při stínění vesmírného záření. [26]

Shrnutí využitých materiálů: [26]

- CFRP stěny: laminované [0/45/90/-45]_S
- Hliníkové díly (slitina 7075-T6)
- Hliníkové koleje: povrchová úprava: Eloxování
- Šroubové spoje: Nerezová ocel, M3 imbus šestihran



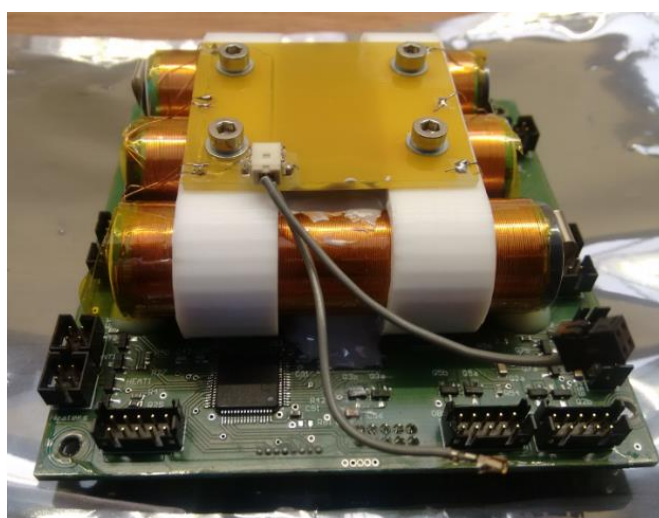
Obr. 18 Nosná konstrukce satelitu UPSat [26]

5.1.2 Elektrický zdrojový systém (EPS)

EPS generuje, ukládá a řídí veškerou elektrickou energii v satelitu. Základním principem je absorbování energie z fotovoltaických článků a následná distribuce k jednotlivým systémům satelitu. V případě nedostatečného množství energie z fotovoltaických článků je možné využít elektrickou energii z baterie. Elektrický zdrojový systém a distribuční systém je složen z těchto hlavních součástí: [26]

- Vysoce účinné fotovoltaické články, připojené k bateriím pomocí převodníků napětí.
- Lithium-polymerové baterie, (3,7 V, 4 Ah)
- Přepínače MOSFET k ovládání výkonu

Celková hmotnost elektrického zdrojového systému (EPS) je 318 g (fotovoltaické články: 22 g, baterie: 46 g, deska: 250 g. [26]



Obr. 19 Základní deska EPS s bateriemi [26]

5.1.3 Systém pro získávání obrazu (IAC)

IAC jakožto sekundární užitečné zatížení slouží k pořizování snímků Země. Systém se skládá ze základní desky DART4460, USB fotoaparátu Ximea MU9PM-MH a objektivu. [26]

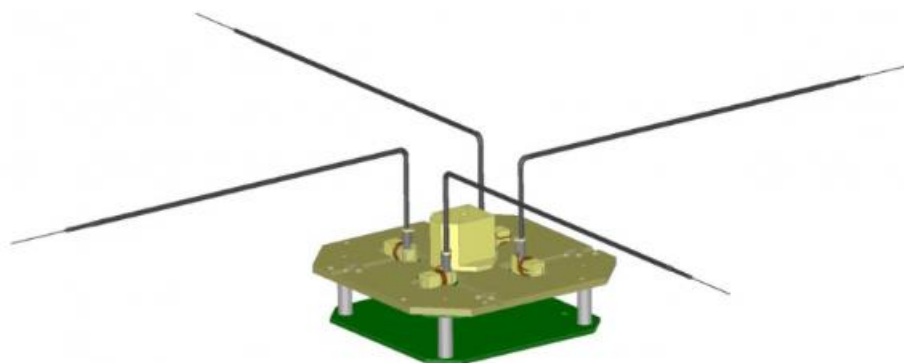


Obr. 20 USB fotoaparát XIMEA [26]

5.1.4 Vědecká jednotka (SU)

Zařízení, které pomocí čtyř jehlových sond měří naindukovaný proud. Ten je přepočítán na napětí a po digitalizaci se výsledek odesílá do systému centrální telemetrie. Umístění přístroje je na přední satelitu z důvodu ovlivnění měření. V případě správné konstrukce vědecké jednotky lze měřit hodnoty proudu v rozsahu od 1 nA do 2 μ A. Vědecká jednotka je složena z: [26]

- jedné desky plošných spojů pro sběr dat
- jedné desky plošných spojů, která funguje jako montážní deska pro sondu
- hliníkové horní desky
- integrovaného emitoru elektronů



Obr. 21 Vědecká jednotka [26]

5.1.5 Systém určování polohy a řízení (ADCS)

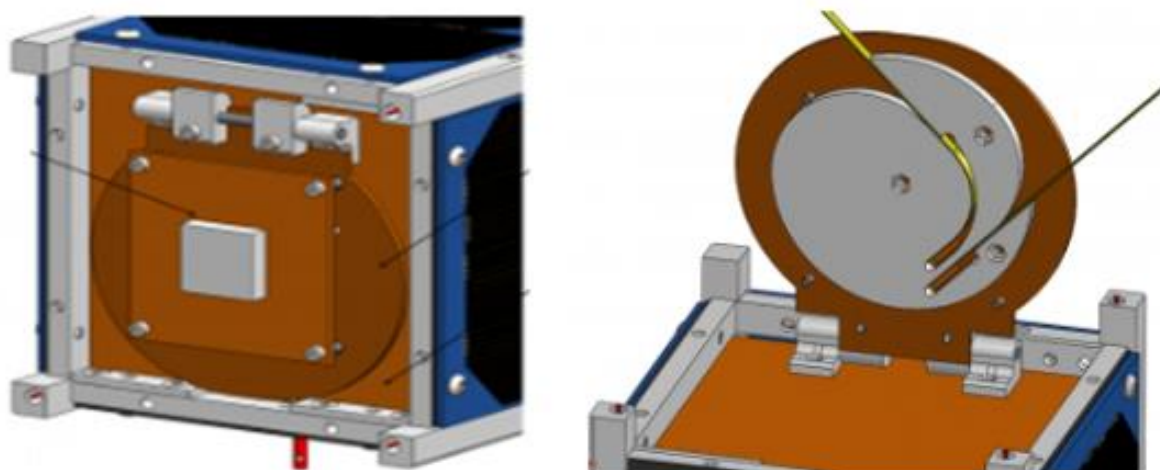
Systém stabilizuje a řídí satelit v požadovaných směrech podle plánu mise. Poloha satelitu je určována a snímána pomocí senzorů polohy, a ovládána pomocí reakčních kol. [26]

5.1.6 Palubní počítačový systém (OBC)

Systém palubního počítače zabezpečuje funkci mozku celého satelitu. Úkolem OBC je kromě zabezpečení řídicích letových funkcí i veškeré rozhodování a monitorování ostatních systémů satelitu. Nejdůležitější součástí OBC systému je mikroprocesor STM32F4. Na základní desce se nachází také systém pro získávání obrazu. Systém rovněž zabezpečuje komunikaci se všemi ostatními systémy satelitu. [26]

5.1.7 Komunikační systém (COMM)

Na základě předchozích úspěšných zkušeností je funkce komunikačního systému založena na čipu CC1120. Původně plánované zdvojení komunikačního systému se nakonec prokázalo jako nevhodné a úspora hmotnosti zvítězila nad spolehlivostí. Součástí komunikačního systému jsou dvě komunikační antény. Délky antén se volí na základě délky vysokofrekvenčních vln. První anténa pro downlink komunikaci (komunikaci ze satelitu na zem) je dlouhá 180 mm, pro pásmo ultra krátkých vln pro frekvenci 433MHz. Druhá pro uplink komunikaci (komunikace ze země k satelitu) měří 610 mm, pro pásmo velmi krátkých vln pro frekvenci 144 MHz. Antény se nachází na opačné straně satelitu než vědecká jednotka. Při finančně nákladných kosmických letech jsou rozměry antén velkou komplikací. Proto je nutné využití otevíracích a výklopných mechanismů. Antény se tak vyklopí až v okamžiku, kdy se satelit nachází na oběžné dráze. [26]



Obr. 22 Výklopný systém antén satelitu [26]

6 Analýza elektrického zdrojového systému (EPS)

6.1 Popis a funkce systému

Aplikace spolehlivostních metod byla provedena na části obvodu elektrického zdrojového systému (EPS), jehož elektrotechnické schéma (Obr. 23) a seznam součástí (Tab. 19) jsou veřejně dostupné na webových stránkách satelitu. Analyzovaná část obvodu zajišťuje napájení komunikační desky a palubního počítače elektrických proudem o nominálním napětí +3,3 VDC. Proudové výstupy na ostatní desky jsou ve schématu připraveny pro případné využití v budoucnosti, zůstávají ale protazím nezapojeny. Rovněž monitor proudu (M8) z regulátoru napětí není zapojen. Úkolem spínaného regulátoru napětí (B2) v obvodu je snížit vstupní napětí +12 VDC z baterie solárního systému satelitu na úroveň napětí potřebnou k napájení jednotlivých desek +3,3 VDC. Funkce regulátoru je umožněna v případě, že napětí na vstupu EN dosáhne úroveň odpovídající logické jedna. Výstupní napětí z regulátoru je nastaveno poměrem hodnot odporů RFB3 a RFB4 na napěťovém děliči. Zvlnění napětí na výstupu z regulátoru je filtrováno pomocí tantalových a keramických kondenzátorů (C41, C71-C73, C79, C84, C85, C87). Napájení pro jednotlivé desky je spínáno pomocí unipolárních tranzistorů (FET). Použity jsou vždy dvojice tranzistorů, a to z důvodu rozdělení proudové zátěže.

Spínaný regulátor implementuje funkci zkratové a nadproudové ochrany, ochranu proti přepětí a podpětí monitorováním vazby (pin VFB) a ochranu proti přehřátí.

Návrh vzorového obvodu, výběr konkrétních typů a parametrů součástek, a výpočet skutečného zatížení součástek není součástí této práce. Snahou bylo zvolit takové součástky, které jsou využívány pro vesmírná zařízení a mají jasně zaručenou úroveň kvality.

Cílem práce bylo postupně provést tyto vybrané spolehlivostní metody:

- Analýza odlehčení součástek (derating)

Analýza má za cíl ověřit navrhnuté součástky tak, aby byla minimalizována možnost překročení jejich maximálních přípustných parametrů. Maximální přípustné parametry uvedené výrobcem budou úmyslně sníženy v souladu se standardem ECSS-Q-ST-30-11C a následně porovnány se skutečnými hodnotami zatížení. Návrh obvodu vyhovuje požadavkům na odlehčení v případě, že žádná z hodnot skutečného zatížení nebude větší než odlehčená hodnota. V opačném případě by kvůli výrobním odchylkám nebo rozptylu ve skutečném zatížení mohlo dojít k přetížení součástek a následné poruše. V takovém případě by se musela vyhodnotit výše rizika a případně zvolit součástka jiná.

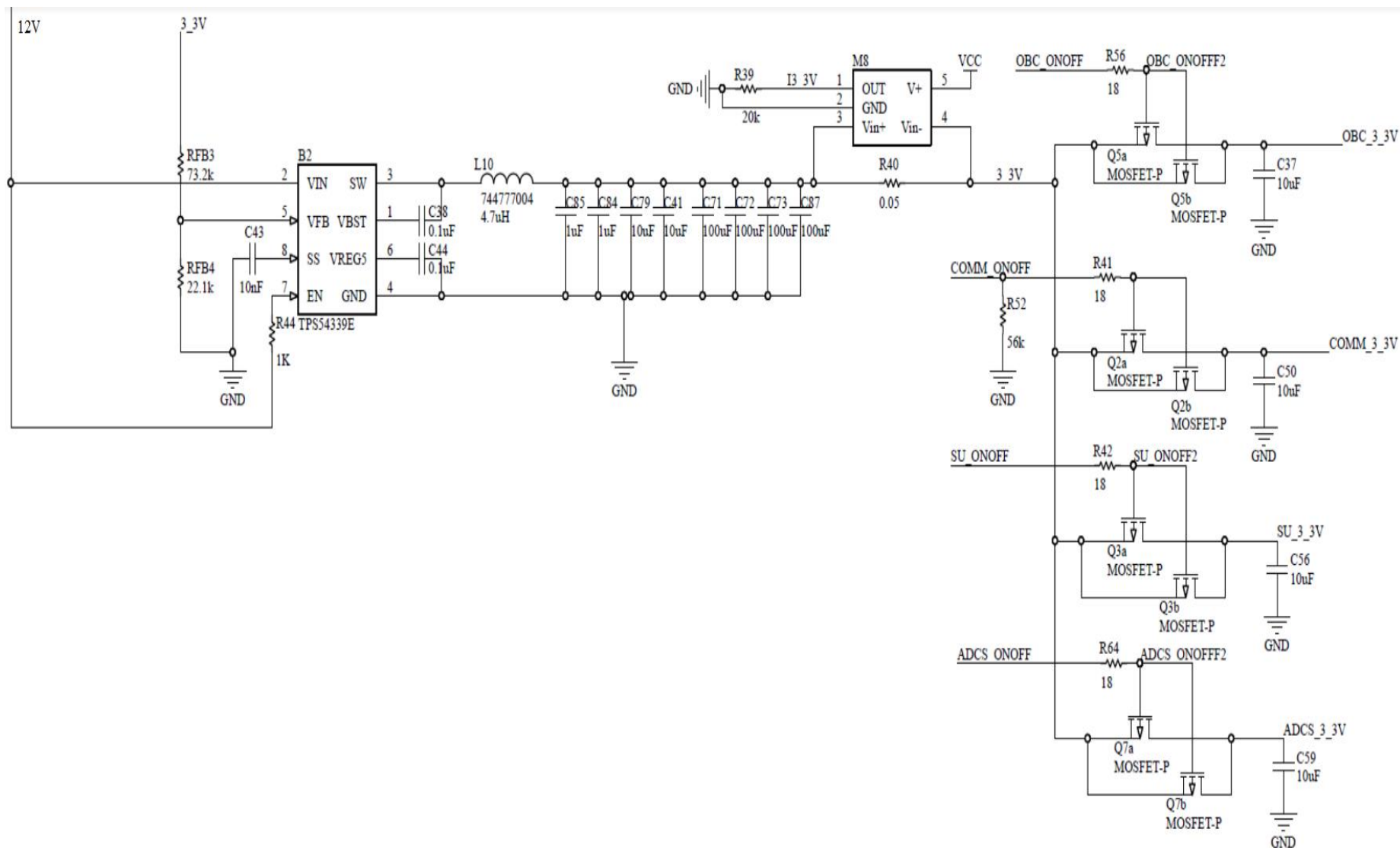
- Analýza bezporuchovosti

Analýza bezporuchovosti má za cíl ověřit, zda pravděpodobnost bezporuchové funkce EPS vypočtena metodou zatížení součástek v souladu s MIL-HDBK-217F, Notice 2 vyhovuje těmto požadavkům:

- 1) Pravděpodobnost bezporuchového provozu EPS desky při aktivním provozu musí být větší než 99,6 % po dobu trvání mise 1,5 let.
- 2) Pravděpodobnost bezporuchového provozu EPS desky při aktivním provozu musí být větší než 95 % po dobu trvání mise 15 let.
- 3) Pravděpodobnost bezporuchového provozu dvou EPS v paralelním zapojení (aktivní/studená záloha) musí být větší než 99,99 % po dobu trvání mise 1,5 let
- 4) Pravděpodobnost bezporuchového provozu dvou EPS v paralelním zapojení (aktivní/studená záloha) musí být větší než 99,6 % po dobu trvání mise 15 let

- Analýza způsobů, důsledků a kritičnosti poruch

Analýza má za cíl analyzovat pravděpodobné poruchy součástek EPS desky, jejich důsledky na lokální úrovni i na úrovni samotného satelitu. Na základě výpočtů intenzit poruch z analýzy bezporuchovosti se určí pravděpodobnost bezporuchovosti všech součástek s ohledem na délku mise. Následně budou uvažované způsoby poruch klasifikovány s ohledem na jejich výslednou kritičnost pro vesmírnou misi. Vše bude nakonec zpracováno do přehledného FMECA formuláře.



Obr. 23 Schéma analyzovaného obvodu EPS [44]

Tab. 19 Seznam součástek nacházejících se v analyzovaném obvodu

Ref. číslo	Součástka	PN
B2	Integrovaný obvod, Regulátor napětí	TPS54339E
M8	Integrovaný obvod, Monitor proudu	5962R0924401VHA
L10	Cívka, 4,3uH, SMD	320100905C4L3M
Q2	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3
Q3	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3
Q5	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3
Q7	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3
C43	Kondenzátor, Keramický, 10 nF, 10 %, 50 V	300904103103KC
C38	Kondenzátor, Keramický, 100 nF, 10 %, 50 V	300904103104KC
C44	Kondenzátor, Keramický, 100 nF, 10 %, 50 V	300904103104KC
C85	Kondenzátor, Keramický, 1 uF, 10 %, 25 V	300904103105KA
C84	Kondenzátor, Keramický, 1 uF, 10 %, 25 V	300904103105KA
C79	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C41	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C37	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C50	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C56	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C59	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX
C71	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK
C72	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK
C73	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK
C87	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK
RFB3	Film rezistor, 73.2k Ohm, 0,125 W	4001023027322B2
RFB4	Film rezistor, 22.1k Ohm, 0,125 W	4001023022212B2
R44	Film rezistor, 1k Ohm, 0,2 W	4001026021001F4
R39	Film rezistor, 20k Ohm, 0,2 W	4001026022002F4
R52	Film rezistor, 56k Ohm, 0,2 W	4001026025602F4
R56	Film rezistor, 18 Ohm, 0,2 W	40010260218R0F4
R41	Film rezistor, 18 Ohm, 0,2 W	40010260218R0F4
R42	Film rezistor, 18 Ohm, 0,2 W	40010260218R0F4
R64	Film rezistor, 18 Ohm, 0,2 W	40010260218R0F4
R40	Film rezistor, 0.05 Ohm, 1 W	400102701R050D

6.2 Analýza odlehčení součástek

Analýza odlehčení obvodu elektrického zdrojového systému (EPS) byla provedena v souladu se standardem ECSS-Q-ST-30-11C. Standard doporučuje parametry a hodnoty odlehčení pro jednotlivé elektrické a elektronické součástky. Význam dané analýzy byl již vysvětlen v kapitole 3.1.

Návrh obvodu vyhovuje požadavkům na odlehčení v případě, že žádná z hodnot skutečného zatížení není větší než odlehčená hodnota. Ve své podstatě se jedná o procentuální vyjádření rezervy vůči maximální přípustné hodnotě uvedené výrobcem. Odlehčené hodnoty musí být vyšší než skutečné provozní hodnoty. Příklad pro použití analýzy pro jednotlivé typy součástek a jejich požadované parametry odlehčení jsou uvedeny v následujícím textu.

6.2.1 Integrovaný obvod

Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.21

- Napájecí napětí: 90 % maximální katalogové hodnoty
- Vstupní napětí: 70 % maximální katalogové hodnoty
- Výstupní proud: 80 % maximální katalogové hodnoty
- Teplota přechodu: 110 °C nebo $T_{\max} - 40$ °C (použije se nižší z hodnot)

6.2.2 Cívka pro spínaný zdroj 4,3 μH

Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.18

- Maximální provozní napětí: 50 % maximální katalogové hodnoty
- Teplota hot-spot: 20 °C pod maximální teplotu

6.2.3 Unipolární tranzistor (FET)

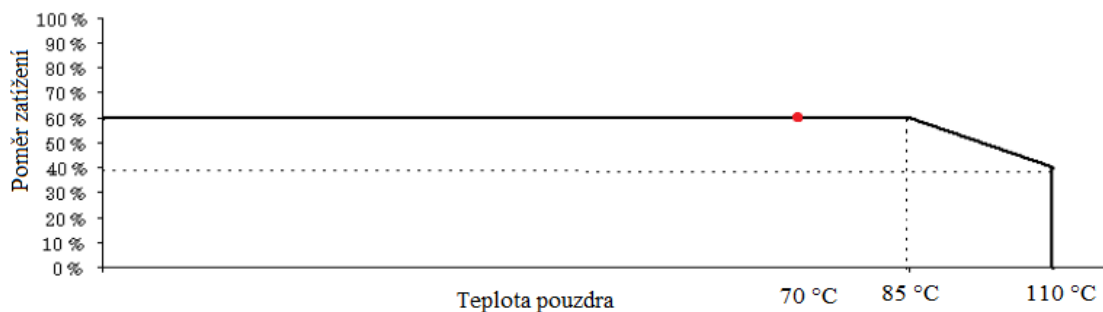
Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.29

- Napětí mezi elektrodami Drain a Source (V_{DS}): 80 % maximální katalogové hodnoty
- Napětí mezi elektrodami Gate a Source (V_{GS}): 75 % maximální katalogové hodnoty
- Výstupní proud: 75 % maximální katalogové hodnoty
- Ztrátový výkon: 65 % maximální katalogové hodnoty
- Teplota přechodu: 110 °C nebo $T_{\max} - 40$ °C (použije se nižší z hodnot)

6.2.4 Keramický kondenzátor

Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.2

- Napětí: pro teplotu pouzdra 70 °C platí odlehčení 60 % z maximální hodnoty

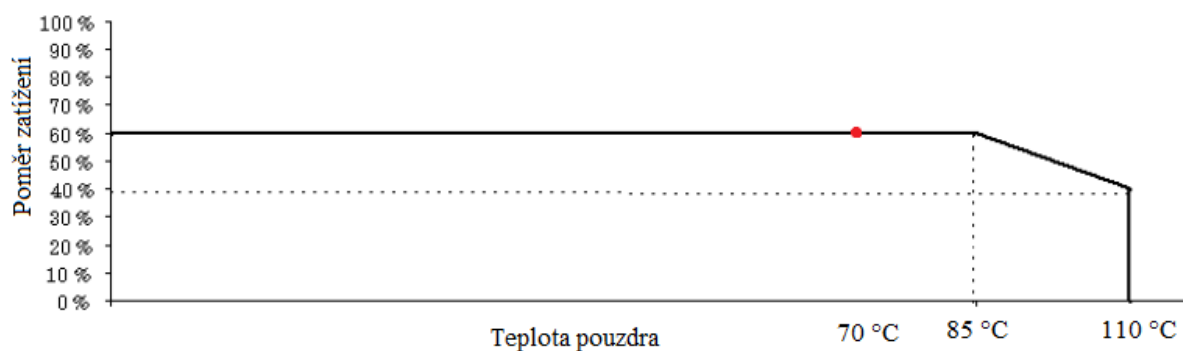


Obr. 24 Křivka odlehčení napětí pro keramický kondenzátor [12]

6.2.5 Tantalový kondenzátor

Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.3

- Napětí: pro teplotu pouzdra 70 °C platí odlehčení 60 % z maximální katalogové hodnoty



Obr. 25 Křivka odlehčení napětí pro tantalový kondenzátor [12]

- Nárazový proud: 75% maximální katalogové hodnoty
- Zvlnění proudu: 50% maximální katalogové hodnoty

6.2.6 Rezistor

Parametry odlehčení dle ECSS-Q-ST-30-11C, kapitola 6.26

- Napětí: 80 % maximální katalogové hodnoty
- Efektivní hodnota výkonu: 50 % (do teploty 85 °C)

Výsledky analýzy odlehčení pro všechny součástky jsou zpracovány v diplomové práci jako Příloha 1.

6.3 Analýza bezporuchovosti

V analýze bezporuchovosti byly vypočítány hodnoty intenzity poruch součástek elektrického zdrojového systému (EPS). Cílem bylo stanovit pravděpodobnost bezporuchové funkce systému po dobu trvání uvažované vesmírné mise a prokázat soulad s požadavky na bezporuchovost funkce systému v kapitole 6.1. Délka vesmírné mise byla uvažována 18 měsíců a 15 let. Tady je patrný rozdíl oproti spolehlivosti v oblasti letecké. Jelikož se jedná o satelit, u kterého se nepředpokládá žádná údržba v průběhu mise, má důležitý vliv na výslednou poruchovost nejenom intenzita poruch, ale také délka vesmírné mise. Pro stanovení intenzit poruch jednotlivých součástek elektrického zdrojového systému byla použita příručka MIL-HDBK-217F, Notice 2. Tyto intenzity poruch byly rovněž použity pro stanovení kritičnosti poruchových stavů součástek v analýze FMEA.

6.3.1 Výpočet intenzit poruch

Pro dosažení správných součinitelů potřebných k výpočtu intenzit poruch byly využity katalogy součástí: [2], [3], [6], [18], [23], [29], [40], [41], [42]. Pomocí těchto katalogů byl stanoven správný typ součástky a určeny další potřebné informace pro odhad součinitelů ovlivňujících intenzitu poruch. Další potřebné hodnoty pro výpočet součinitelů byly využity z tabulek maximálních a skutečných hodnot v Příloha 2. Pro všechny analyzované součásti bylo uvažováno vesmírné prostředí (S_F). Všechny součástky jsou vyráběny více než 2 roky. Bylo snahou zvolit součástky o známé úrovni kvality, které jsou vhodné pro vesmírné prostředí a mise v něm. Většina součástek má úroveň kvality klasifikovanou podle jiné normy, než byla využívána. V takovémto případě bylo nutné jednotlivé označení úrovně kvality převést na odpovídající ekvivalentní označení.

Průběh výpočtů bude dokumentován pouze pro jednu součástku z dané skupiny. U ostatních součástí z dané skupiny je postup identický a výsledky jsou zpracovány v tabulce, která je umístěna v diplomové práci jako Příloha 2.

6.3.1.1 Integrovaný obvod B2

$$\text{Vzorec pro výpočet:} \quad \lambda_p = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L, \quad \text{poruch}/10^6h \quad (6.1)$$

Tab. 20 Součinitele pro výpočet intenzity poruch regulátoru napětí dle MIL-HDBK-217F-2 [31]

Součinitel ovlivňující intenzitu poruch	Hodnota součinitele	Poznámka
Součinitel složitosti integr. obvodu C_1	0,01	Kapitola 5.1 v [31], MOS Linear, do 100 tranzistorů
Součinitel složitosti integr. obvodu C_2	0,0013	Kapitola 5.9 v [31], 8 pinů
Teplotní součinitel π_T	6,9	Kapitola 5.8 v [31], Linear, Teplota přechodu = 84,85 °C dle Příloha 2
Součinitel prostředí π_E	0,5	Kapitola 5.10 v [31], prostředí: SF (Space, Flight)
Součinitel zkušenosti π_L	1,0	Kapitola 5.10 v [31], více než 2 roky vyráběná součástka
Součinitel kvality π_Q	1,0	Kapitola 5.10 v [31], neznámá úroveň kvality, hodnota podle ANSI/VITA 51.1-2008 [1]

$$\lambda_p = 6,962 \cdot 10^{-2} \quad (6.2)$$

6.3.1.2 Cívka pro spínaný zdroj L10

Vzorec pro výpočet: $\lambda_p = \lambda_b \pi_T \pi_Q \pi_E, \text{ poruch}/10^6 h$ (6.3)

Tab. 21 Součinitele pro výpočet intenzity poruch cívky dle MIL-HDBK-217F-2 [31]

Součinitel ovlivňující intenzitu poruch	Hodnota součinitele	Poznámka
Základní intenzita poruch λ_b	0,0003	Kapitola 11.2 v [31], Fixed type
Teplotní součinitel π_T	2,16	Kapitola 11.2 v [31], Teplota Hot-Spot = 90,48 °C dle Příloha 2
Součinitel kvality π_Q	0,3	Kapitola 11.2 v [31], úroveň kvality dle ECSS „C“ je ekvivalentní s úrovní kvality „P“ dle MIL-HDBK-217F, viz. Tab. 11
Součinitel prostředí π_E	0,5	Kapitola 11.2 v [31], prostředí: SF (Space, Flight)

$$\lambda_p = 9,735 \cdot 10^{-6} \text{ poruch}/10^6 h \quad (6.4)$$

6.3.1.3 Unipolární tranzistor Q2a

Vzorec pro výpočet: $\lambda_p = \lambda_b \pi_T \pi_A \pi_Q \pi_E, \text{ poruch}/10^6 h$ (6.5)

Tab. 22 Součinitele pro výpočet intenzity poruch tranzistoru dle MIL-HDBK-217F-2 [31]

Součinitel ovlivňující intenzitu poruchy	Hodnota součinitele	Poznámka
Základní intenzita poruch λ_b	0,012	Kapitola 6.4 v [31], typ tranzistoru MOSFET
Teplotní součinitel π_T	2,4	Kapitola 6.4 v [31], Teplota přechodu = 71,75 °C dle Příloha 2
Aplikační součinitel π_A	0,7	Kapitola 6.4 v [31], Spínání signálů
Součinitel kvality π_Q	0,7	Kapitola 6.4 v [31], úroveň kvality dle výrobce „JANS“ je vyšší než úrovně ve příručce, volíme nejvyšší JANTXV
Součinitel prostředí π_E	0,5	Kapitola 6.4 v [31], prostředí: SF (Space, Flight)

$$\lambda_p = 7,060 \cdot 10^{-3} \text{ poruch}/10^6 h \quad (6.6)$$

6.3.1.4 Keramický kondenzátor C43

Vzorec pro výpočet: $\lambda_p = \lambda_b \pi_T \pi_C \pi_V \pi_{SR} \pi_Q \pi_E, \text{ poruch}/10^6 h$ (6.7)

Tab. 23 Součinitele pro výpočet intenzity poruch keramického kondenzátoru dle MIL-HDBK-217F-2 [31]

Součinitel ovlivňující intenzitu poruchy	Hodnota součinitele	Poznámka
Základní intenzita poruch λ_b	0,002	Kapitola 10.1. v [31], CDR typ
Teplotní součinitel π_T	5,98	Kapitola 10.1. v [31], Teplota pouzdra = 70 °C dle Příloha 2
Součinitel kapacity π_C	0,661	Kapitola 10.1. v [31], kapacita 0,01uF dle Příloha 2
Součinitel napětí π_V	1,064	Kapitola 10.1. v [31], S (skutečné napětí/maximální napětí) = 0,24
Součinitel odporu π_{SR}	1,0	Kapitola 10.1. v [31], vztahuje se pouze na tantalové kondenzátory
Součinitel kvality π_Q	0,3	Kapitola 10.1. v [31], úroveň kvality dle ECSS „C“ je ekvivalentní s úrovní kvality „P“ dle MIL-HDBK-217F, viz. Tab. 11
Součinitel prostředí π_E	0,5	Kapitola 10.1 v [31], prostředí: SF (Space, Flight)

$$\lambda_p = 1,261 \cdot 10^{-3} \text{ poruch}/10^6 h \quad (6.8)$$

6.3.1.5 Rezistor

Vzorec pro výpočet: $\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E, \text{ poruch}/10^6 h$ (6.9)

Tab. 24 Součinitele pro výpočet intenzity poruch rezistoru dle MIL-HDBK-217F-2 [31]

Součinitel ovlivňující intenzitu poruchy	Hodnota součinitele	Poznámka
Základní intenzita poruch λ_b	0,0037	Kapitola 9.1 v [31], RM typ
Teplotní součinitel π_T	1,5	Kapitola 9.1 v [31], Teplota pouzdra = 70 °C dle Příloha 2
Součinitel výkonu π_P	1,0	Kapitola 9.1 v [31], Ztrátový výkon = 1 W z Tab. 32
Součinitel výkonového zatížení π_S	0,88	Kapitola 9.1 v [31], S = 0,2 z dle Příloha 2
Součinitel kvality π_Q	0,3	Kapitola 9.1 v [31], úroveň kvality dle ECSS „C“ je ekvivalentní s úrovní kvality „P“ dle MIL-HDBK-217F-2, viz. Tab. 11
Součinitel prostředí π_E	0,5	Kapitola 9.1 v [31], prostředí: SF (Space, Flight)

$$\lambda_p = 7,389 \cdot 10^{-4} \text{ poruch}/10^6 h \quad (6.10)$$

Výpočty a výsledky pro všechny součástky analyzovaného obvodu jsou uvedeny v příloze k této diplomové práci. Pro výpočet intenzity poruch zkoumaného obvodu byl využit výpočtový vzorec:

$$\lambda_s = \sum_{i=1}^N \lambda_i \quad (6.11)$$

Výsledná intenzita poruch zkoumaného systému (duty cycle 100 %):

$$\lambda_{op} = 1,594 \cdot 10^{-7} \left(\frac{\text{poruch}}{h} \right) \quad (6.12)$$

Při výpočtu celkové intenzity poruch zkoumaného obvodu je uvažováno sériové zapojení, jelikož žádná součástka není vyloženež zálohována. V takovém případě se předpokládá, že selhání jedné součástky má kritické důsledky pro vesmírnou misi. V případě nedostatečné výsledné pravděpodobnosti bezporuchové funkce nebo v případě potřeby přesnějšího odhadu by bylo nutné použít některou z podrobnějších modelovacích metod (např. FMEA). Při takových metodách je ale nutná dokonalá znalost analyzovaného obvodu, nebo v případě některých poruch rovněž testování injektováním poruch do modelu nebo prototypu desky. Pro příklad lze uvést blok filtračních kondenzátorů (C85, C84, C79, C41, C71, C72, C73, C87). Jejich účelem je vyhladit zvlněné napětí vznikající spínáním regulátoru. Jednotlivé poruchy kondenzátorů s nižší kapacitou by neměly mít vliv na funkci satelitu, ale kdyby porucha nastala

u více z nich, mohlo by dojít ke kritickému zvlnění napětí na výstupu, s možností překročení návrhových hodnot napájených desek. V případě detailní analýzy by bylo nutné znát kritické hodnoty zvlnění napětí, a na základě toho určit, jaká kombinace poruch kondenzátorů by ještě byla dostatečná pro bezporuchovou funkci satelitu.

6.3.2 Výpočet pravděpodobnosti bezporuchového provozu sériového systému

1) Pravděpodobnost, že v systému nedojde k žádné poruše v průběhu trvání vesmírné mise o délce $t = 1,5$ let ($\approx 13\,140$ hodin).

$$R_{op}(t) = \exp(-\lambda_{op} \cdot t) \quad (6.13)$$

$$R_{op}(13140) = \exp(-1,594 \cdot 10^{-7} \cdot 13140) \quad (6.14)$$

Pravděpodobnost bezporuchovosti systému pro aktivní režim:

$$R_S = R_{op}(13140) = 0,997907 \quad (6.15)$$

2) Pravděpodobnost, že v systému nedojde k žádné poruše v průběhu trvání vesmírné mise o délce $t = 15$ let ($\approx 131\,400$ hodin).

$$R_{op}(131400) = \exp(-1,594 \cdot 10^{-7} \cdot 131400) \quad (6.16)$$

$$R_S = R_{op}(131400) = 0,979268 \quad (6.17)$$

6.3.3 Výpočet pravděpodobnosti bezporuchového provozu paralelního systému

V tomto případě uvažujeme paralelní zapojení dvou obvodů EPS. Jeden jako primární (aktivní) a druhý jako záložní (pasivní). Pro záložní obvod se předpokládá jeho spuštění až při selhání primárního, a proto je nutné přepočítat intenzity poruch právě pro neoperační režim.

Tab. 25 Poměr intenzity poruch při aktivním a pasivním režimu [39]

Typ součástky	Převodový součinitel pro vesmírné prostředí
Integrovaný obvod	0,1
Dioda	0,2
Tranzistor	0,2
Kondenzátor	0,2
Rezistor	0,5
Spínač	0,8
Deska plošných spojů	0,08
Transformátor, Cívka	0,5

Výsledná intenzita poruch analyzovaného obvodu (duty cycle 0 %)

$$\lambda_{nop} = 7,972 \cdot 10^{-8} \left(\frac{poruch}{h} \right) \quad (6.18)$$

3) Pravděpodobnost, že v systému nedojde k žádné poruše v průběhu trvání vesmírné mise o délce $t = 1,5$ let ($\approx 13\,140$ hodin).

Pravděpodobnost bezporuchové funkce záložního obvodu v průběhu trvání mise:

$$R_{nop}(t) = \exp(-\lambda_{nop} \cdot t) \quad (6.19)$$

$$R_{nop}(13140) = \exp(7,972 \cdot 10^{-8} \cdot 13140) \quad (6.20)$$

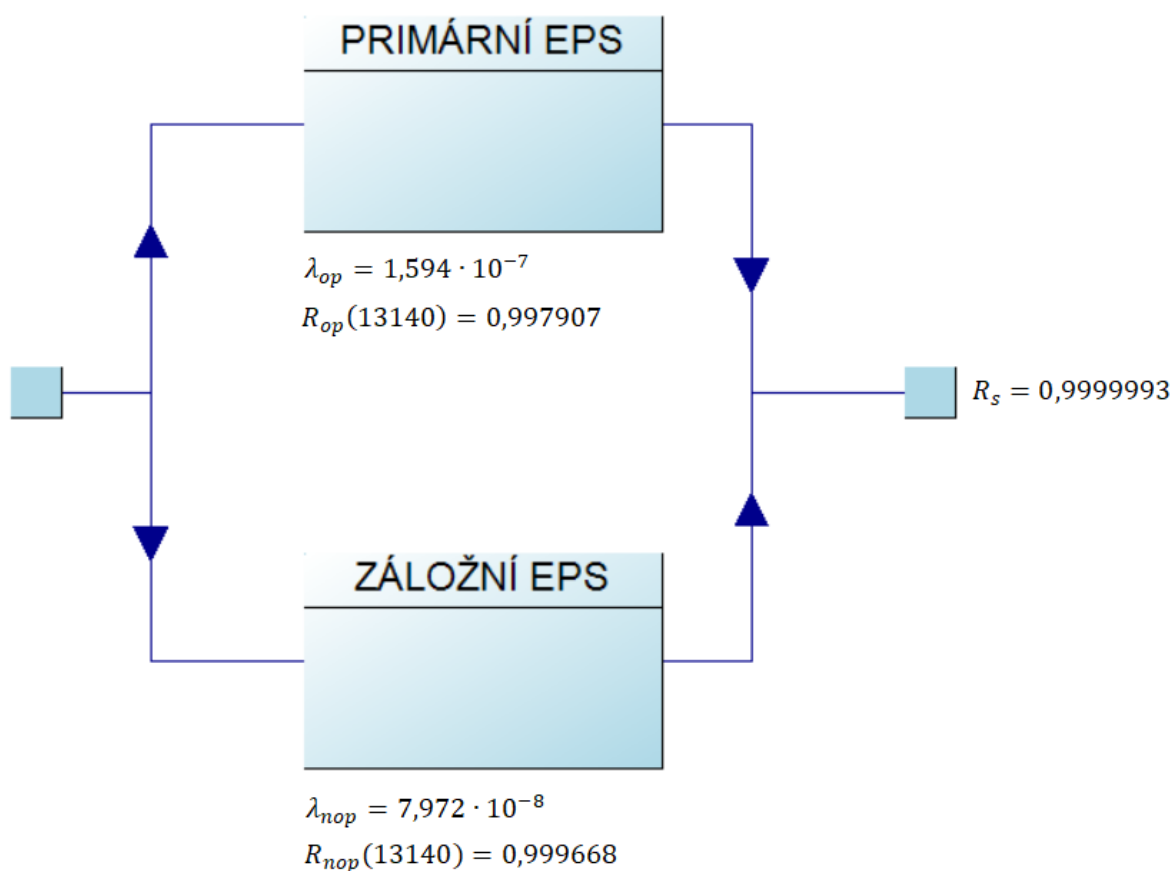
$$R_{nop}(13140) = 0,999668 \quad (6.21)$$

Výsledná hodnota pravděpodobnosti bezporuchové funkce paralelního systému byla dopočítána pomocí vzorce pro paralelní strukturu.

$$R_s = R_{op} + R_{nop} - (R_{op} \cdot R_{nop}) \quad (6.22)$$

Pravděpodobnost bezporuchovosti celého systému:

$$R_s = 0,9999993 \quad (6.23)$$



Obr. 26 Bezporuchovost paralelního systému pro misi ($t=1,5$ let)

4) Pravděpodobnost, že v systému nedojde k žádné poruše v průběhu trvání vesmírné mise o délce $t = 15$ let ($\approx 131\,400$ hodin).

Pravděpodobnost bezporuchové funkce záložního obvodu v průběhu trvání mise:

$$R_{nop}(t) = \exp(-\lambda_{nop} \cdot t) \quad (6.24)$$

$$R_{nop}(131400) = \exp(7,972 \cdot 10^{-8} \cdot 131400) \quad (6.25)$$

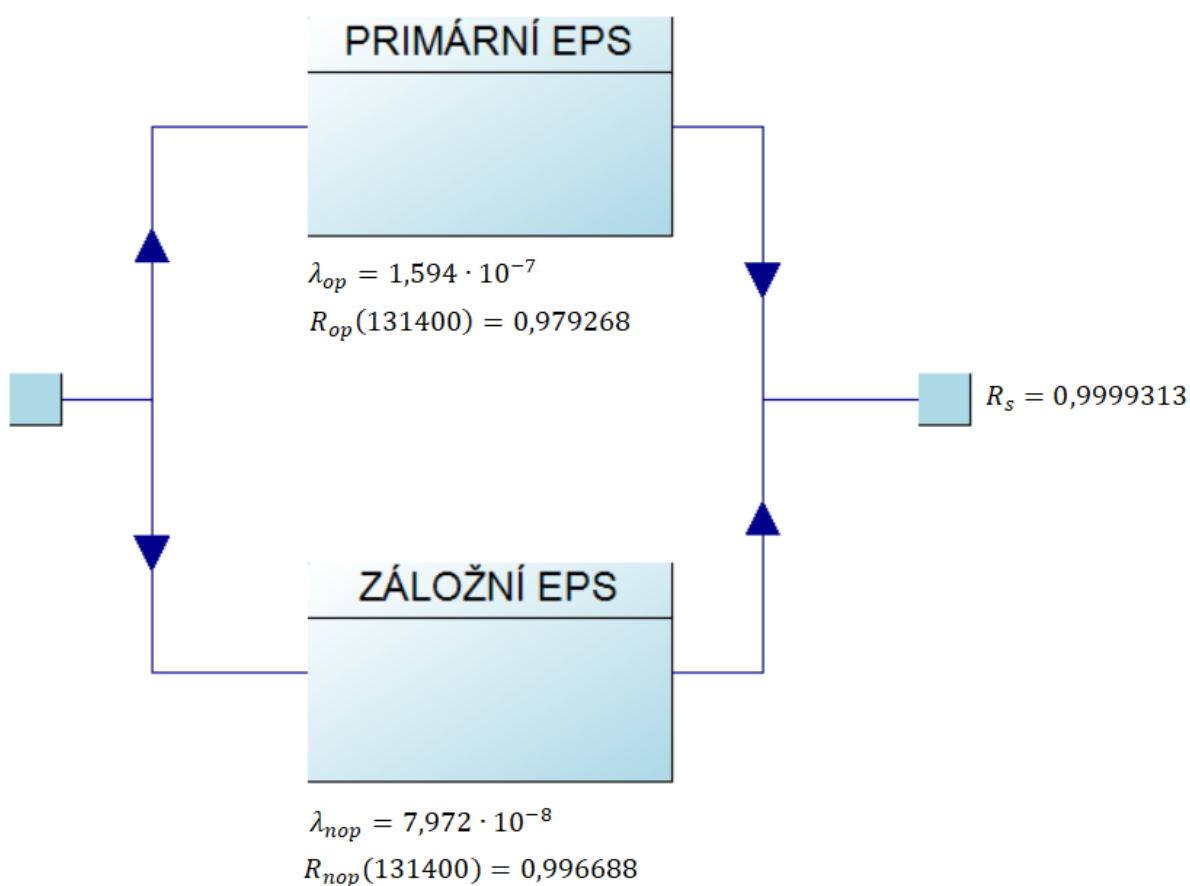
$$R_{nop}(131400) = 0,996688 \quad (6.26)$$

Výsledná hodnota pravděpodobnosti bezporuchové funkce paralelního systému byla dopočítána pomocí vzorce pro paralelní strukturu.

$$R_s = R_{op} + R_{nop} - (R_{op} \cdot R_{nop}) \quad (6.27)$$

Pravděpodobnost bezporuchovosti celého systému:

$$R_s = 0,9999313 \quad (6.28)$$



Obr. 27 Bezporuchovost paralelního systému pro misi ($t=15$ let)

6.4 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)

FMECA má za cíl analyzovat pravděpodobné poruchové stavy vybraného obvodu desky elektrické zdrojové soustavy (EPS) na komponentní úrovni, stanovit jejich důsledky na lokální úrovni, úrovni následující vyšší i na úrovni samotného satelitu. Následně jsou s využitím intenzit poruch z analýzy bezporuchovosti klasifikovány poruchy jednotlivých součástek s ohledem na jejich kritičnost pro vesmírnou misi. Analýza byla provedena v souladu se standardem ECSS-Q-ST-30-02C. Výstupem FMECA je pracovní formulář obsahující všechny potřebné informace o zkoumaných součástkách. Pracovní formulář je zpracován v diplomové práci jako Příloha 3, v Tab. 26 je uveden pouze výstřížek znázorňující vzhled pracovního formuláře.

Tab. 26 Výstřížek pracovního formuláře FMECA

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: Satelit UPSat				Funkce: Regulace napětí +3,3 VDC			Datum: 16.5.2020									
Modul: Elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců			Vypracoval: Marek Horčíčka									
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. důsledku poruchy β	Intenzita způsobu poruchy λ_{fm} (1/hodina)	Pravděp. způsobu poruchy	PN	C N
FM1	B2	Regulátor napětí, step-down, 3,3V	Ztráta výstupu	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,52	1,0	3,620E-08	4,76E-04	2	6

6.4.1 Referenční a identifikační číslo

Všechny součástky musí mít ve formuláři přiřazené referenční číslo, kterým jsou označeny ve schématu. Identifikačním číslem musí být označen každý řádek (způsob poruchy). Čísla slouží pro jednoduchou a rychlou orientaci v ve formuláři a vyhodnocování analýzy.

6.4.2 Způsob poruchy a jeho pravděpodobnost

Dalším krokem je vymezení, jakým způsobem může k poruchám součástky dojít. V práci byly pro elektronické součástky uvažovány tyto způsoby poruch:

Tab. 27 Pravděpodobnosti způsobů poruchy [35]

Součástka	Způsob poruchy	Pravděpodobnost způsobu poruchy
Rezistor	Přerušení	1
Kondenzátor	Zkrat	0,63
	Přerušení	0,37
Cívka, Induktor	Zkrat	0,5
	Přerušení	0,5
Tranzistor	Zkrat	0,73
	Přerušení	0,27
Integrovaný obvod, lineární	Ztráta výstupu	0,77
	Nesprávný výstup	0,23
Integrovaný obvod, napájení	Ztráta výstupu	0,52
	Nesprávný výstup	0,48

Dokument [35] popisuje kromě typických způsobů poruch rovněž poruchy vedoucí k degradaci parametrů. Degradace parametrů není v této analýze uvažována, a to z důvodu, že u vesmírných projektů se standartně provádí analýza nejhoršího možného případu. Jednotlivé pravděpodobnosti způsobů poruchy jsou z toho důvodu přerozděleny mezi ostatní způsoby poruch takovým způsobem, aby byl pro každou součástku roven 1 (100 %). Jako příklad lze uvést keramický kondenzátor, u kterého byla pravděpodobnost poruchy vedoucí na degradaci parametrů přerozdělena rovnoměrně mezi zkrat a přerušení.

6.4.3 Důsledky poruchy na jednotlivých úrovních

Rozdělení úrovní důsledků bylo následujícím způsobem:

- Lokální důsledek – důsledek poruchy, který má vliv na konkrétní danou součástku nebo součástky nebo analyzovaný obvod
- Důsledek na další úrovni – důsledek poruchy, který má vliv na funkci napájených desek palubního počítače a komunikačního systému
- Konečný důsledek – důsledek poruchy, který má vliv na funkci satelitu a úspěšnost jeho mise

6.4.4 Hodnocení úrovně závažnosti

Na základě konečného důsledku se určuje kategorie závažnosti dle 4 úrovní:

- 1 – Katastrofické
- 2 – Kritické
- 3 – Závažná
- 4 – Nezávažná

Jelikož se jedná o vědecký nanosatelit, klasifikace s katastrofickými důsledky pro spolehlivost není na této úrovni definována viz Tab. 12. Tudíž jako nejhorší klasifikace závažnosti důsledku je uvažována kategorie kritická, kdy hrozí ztráta funkce satelitu a tím i ztráta celé mise. Klasifikace závažná se vztahuje na veškeré omezení a degradování funkcí systému, u kterého se neočekává úplné ohrožení funkcí satelitu. Klasifikace nezávažná zahrnuje veškeré poruchy, u kterých se nepředpokládá omezující ovlivnění funkčnosti satelitu. Do této kategorie patří také části obvodu, které nejsou zapojeny. K hodnocení úrovně závažnosti jsou v souladu s kapitolou 3.4. přidány přípony.

6.4.5 Přiřazení faktoru závažnosti SN

Faktor závažnosti byl přiřazen na základě kategorie závažnosti viz. Tab. 13.

6.4.6 Detekce nebo projev poruchy

Uvádí se způsob detekce způsobu poruchy nebo její vnější projev v případě, že detekce není implementována.

6.4.7 Kompenzace poruchy

Uvádí se způsob kompenzace poruchy v případě, že je implementováno zálohování.

6.4.8 Pravděpodobnost důsledku poruchy

Uvádí se hodnota pravděpodobnosti důsledku poruchy v intervalu 0 až 1. Jako příklad lze uvést pravděpodobnost, že v důsledku nesprávné funkce napájecího zdroje dojde k přepětí nebo podpětí na výstupu zařízení (v tomto případě uvažováno $\beta = 0,5$).

6.4.9 Intenzita způsobu poruchy

Hodnoty intenzity poruch pro jednotlivé součástky analyzovaného obvodu byly již vypočítány v analýze bezporuchovosti. Pouze bylo nutné přerozdělit tyto hodnoty vzhledem ke způsobům poruchy a pravděpodobnosti důsledků poruchy následujícím způsobem:

$$\lambda_{fm} = \lambda_{op}\alpha\beta \quad (6.29)$$

6.4.10 Pravděpodobnost způsobu poruchy

Pravděpodobnost způsobu poruchy součástky po definovanou dobu mise byla vypočítána na základě intenzity poruch a délky mise následovně:

$$Q_i(t) = 1 - \exp(-\lambda_i t) \quad (6.30)$$

6.4.11 Přiřazení faktoru pravděpodobnosti PN

Pro zjištění faktoru kritičnosti CN je důležité znát také faktor pravděpodobnosti. Dané číslo vyjadřuje pravděpodobnostní interval nastoupení poruchové stavu dle Tab. 14.

6.4.12 Přiřazení faktoru kritičnosti CN

Cílem analýzy kritičnosti, která je součástí FMECA je odhalit kritické prvky systému. Jedná se především o způsoby poruch a součástky, jenž mají analýzou přiřazené hodnocení závažnosti s kritickým nebo závažným důsledkem pro misi, a zároveň nejsou zálohovány (2SP, 3SP). Toto však není jediný faktor určující kritický prvek v systému. Důležitou roli zde hraje také pravděpodobnost nastoupení způsobu poruchy součástky. Právě kombinace těchto dvou faktorů určuje výsledný faktor kritičnosti, díky kterému lze dle matice kritičnosti Tab.15 odhalit, zda bude daný prvek kritický či nikoliv.

ZÁVĚR

Diplomová práce popisuje standardy a metody používané k zajištění spolehlivosti a bezpečnosti kosmických prostředků. V úvodní části diplomové práce je shrnutí základní vesmírné techniky satelitů a příslušné standardizace právě pro oblast kosmického prostředí.

Následující teoretické kapitoly práce se detailně věnují oblastem spolehlivosti a bezpečnosti vesmírných prostředků.

V kapitole věnované spolehlivosti jsou popsány jednotlivé analýzy spolehlivosti v souladu se standardem ECSS-Q-ST-30: analýza odlehčení součástek (derating), analýza nejhoršího případu (WCA), analýza bezporuchovosti a analýza způsobů, důsledků a kritičnosti poruch (FMECA).

Kapitola popisující oblast bezpečnosti je uvedena pouze okrajově, a to z důvodu, že v případě nepilotovaných misí neexistují důvody pro provedení analýz funkční bezpečnosti. V těchto případech je bezpečnost řešena pouze jako součást ochrany pozemního personálu před zraněním, nebo samotného zařízení před poškozením.

V praktické části byly jednotlivé spolehlivostní metody aplikovány na obvod elektrického zdrojového systému (EPS). Z analýz popsaných v kapitole věnované spolehlivosti vesmírných prostředků byly postupně aplikovány analýza odlehčení součástek, analýza bezporuchovosti a analýza způsobů, důsledků a kritičnosti součástek.

Analýza odlehčení součástek, která ověřila správnost použitých součástek v analyzovaném obvodu. Postupovalo se v souladu se standardem ECSS-Q-ST-30-11C. Maximální parametry součástek, které zaručuje výrobce, byly na základě požadavků standardu sníženy a následně porovnány se skutečnými provozními hodnotami. Tímto způsobem byla úspěšně ověřena vhodnost všech navržených elektronických součástek.

V analýze bezporuchovosti byly vypočítány hodnoty intenzit poruch pro každou součástku analyzovaného obvodu. Dále byla ověřena pravděpodobnost bezporuchové funkce desky elektrického zdrojového systému (EPS) pro sériové i paralelní zapojení pro vesmírné mise o délce 1,5 a 15 let. Všechny požadavky na pravděpodobnost bezporuchové funkce byly úspěšně splněny.

V analýze způsobů, důsledků a kritičnosti poruch (FMECA) byly využity výsledky analýzy bezporuchovosti. Byl vypracován přehledný pracovní formulář obsahující pravděpodobné způsoby poruch elektronických součástek, popsány jejich důsledky na různých úrovních a ohodnocena kritičnost každého způsobu poruchy. Kritické elektronické součástky byly identifikovány a označeny v souladu s požadavky matice kritičnosti. Případná úprava návrhu obvodu by záležela především na požadavcích zadavatele a provozovatele satelitu.

Vzhledem k tomu, že se u satelitu po jeho vypuštění nepředpokládají žádné opravy, je jedním z kritických parametrů spolehlivosti délka mise. V případě poruchy během naplánované mise zde není možné provést jakékoliv opravy, což může vést až k úplnému selhání mise bez možnosti obnovení funkcí satelitu. V tom spočívá i největší rozdíl v přístupu ke spolehlivosti a bezpečnosti u kosmické techniky a civilního letectví, kdy je možné po každém přistání nebo alespoň do definované doby (omezené odbavení letounu) provést na dotčeném zařízení opravu nebo výměnu.

Dalším rozdílem ve srovnání s civilním letectvím jsou některá specifika v použití FMEA pro oblast kosmické techniky. Například zaužívané hodnocení konečného důsledku bez ohledu na

možnou detekci nebo kompenzaci poruchy, použití přípon k hodnocení závažnosti důsledků atd. Navíc jsou v případě civilního letectví analýzy jako např. FMEA a FTA zaměřeny hlavně na bezpečnost, a to z důvodu dopadů poruch na letovou posádku nebo cestující. Analýzy spolehlivosti jsou v tomto případě prováděny pouze okrajově (MTBF), nebo používány jako vstupy pro analýzy bezpečnosti.

ZDROJE

- [1] ANSI/VITA 51.1. *American National Standard for Reliability Prediction MIL-HDBK-217 Subsidiary Specification*. American National Standards Institute, 2008.
- [2] AVX [online katalogový list]. *Space Level BME X7R MLCC*. [cit.23.6.2020]. Dostupné z: <http://datasheets.avx.com/SpaceBME.pdf>
- [3] AVX [online katalogový list]. *TAJ ESCC Tantalum Capacitors*. [cit.23.6.2020]. Dostupné z: http://datasheets.avx.com/TAJ_ESCC.pdf
- [4] CSO. Standardy ECSS. *Czech Space Office* [online]. 27.10.2015 [cit. 2020-06-22]. Dostupné z: <https://www.czechspace.cz/cs/standardy-ecss>
- [5] ČSN IEC 60050-192. *Mezinárodní elektrotechnický slovník - Část 192: Spolehlivost*. Praha: Český normalizační institut, 2008. Třídící znak: 330050.
- [6] DSCC [online katalogový list]. *Standard Microcircuit Drawing*. 1997 [cit. 23.6.2020]. Dostupné z: <https://www.datasheets360.com/pdf/-2738009284672793278>
- [7] ECSS. Document Tree. *European Cooperation for Space Standardization* [online]. 19.12.2019 [cit. 2020-06-22]. Dostupné z: <https://ecss.nl/standards/ecss-document-tree-and-status/>
- [8] ECSS-Q-HB-30-01A. *Worst case analysis*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 14.1.2011.
- [9] ECSS-Q-ST-30. *Dependability*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 6.3.2009.
- [10] ECSS-Q-ST-30-02C. *Failure modes, effects (and criticality) analysis (FMEA/FMECA)*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 6.3.2009.
- [11] ECSS-Q-ST-30-08A. *Components reliability data sources and their use*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 14.1.2011.
- [12] ECSS-Q-ST-30-11C Rev 1. *Derating - EEE components*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 4.10.2011
- [13] ECSS-Q-ST-40. *Hazard analysis*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 15.11.2008.
- [14] ECSS-Q-ST-40. *Safety*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 6.3.2009.
- [15] ECSS-Q-TM-30-12A. *End-of-life parameter drifts - EEE components*. 2200 AG Noordwijk, The Netherlands: ESA Requirements and Standards Division, 12.10.2010.
- [16] ESA. Dependability. *European Space Agency* [online]. n.d. [cit. 2020-06-23]. Dostupné z: http://www.esa.int/Enabling_Support/Space_Engineering_Technology/Dependability
- [17] ESA. Effective Reliability Prediction for Space Applications. *European Space Agency* [online]. 2016 [cit. 2020-06-23]. Dostupné z: https://www.reliability.space/app/download/14847209524/ESA_WhitePaper_2016.pdf?t=1553418408
- [18] ESCC [online katalogový list]. *ESCC Detail Specification No.40001/027*. 2018 [cit.23.6.2020]. Dostupné z: <http://escies.org/escs-specs/published/4001027.pdf>

- [19] EverySpec. About EverySpec. *EverySpec* [online]. c2009 - 2020 [cit. 2020-06-22]. Dostupné z: <http://everyspec.com/specifications-about.php>
- [20] FORTESCUE, Peter, Graham SWINERD a John STARK. *Spacecraft Systems Engineering*. 4th ed. New York: Wiley, 2011. ISBN 978-0-470-75012-4.
- [21] HOLUB, Rudolf a Zdeněk VINTR. *Spolehlivost letadlové techniky* [online]. Brno-VUT FSI, 2001.
- [22] InetDaemon. Satellite Orbits. *InetDaemon.Com* [online]. 19.5.2018 [cit. 2020-06-22]. Dostupné z: <https://www.inetdaemon.com/tutorials/satellite/orbits/>
- [23] International Rectifier [online katalogový list]. *Radiation Hardened Power Mosfet Surface Mount*. 2015 [cit.23.6.2020]. Dostupné z: <https://www.datasheets360.com/pdf/7541771621025660241>
- [24] KREBS, Gunter. UPSat (QB50 GR02). *Gunter's Space Page* [online]. 11.12.2017 [cit. 2020-06-23]. Dostupné z: https://space.skyrocket.de/doc_sdat/upsat.htm
- [25] LENERTZ, Brian A. a spol. *Electrical Design Worst-Case Circuit Analysis: Guidelines and Draft Standard (REV A)*. El Segundo, CA: Aerospace, Assuring Space Mission Success, 2013.
- [26] LIBRE SPACE FOUNDATION. *UPSat* [online]. c2016 [cit. 2020-06-23]. Dostupné z: <https://upsat.gr>
- [27] LOFF, Sarah, ed. CubeSats Overview. *NASA* [online]. 14.2.2018 [cit. 2020-06-23]. Dostupné z: https://www.nasa.gov/mission_pages/cubesats/overview
- [28] MAJER, Dušan. Malý průvodce po oběžných drahách. *Kosmonautix.cz* [online]. 11.2.2013 [cit. 2020-06-23]. Dostupné z: <https://www.kosmonautix.cz/2013/02/maly-pruvodce-po-obeznych-drahach>
- [29] MicroSpire [online katalogový list]. *SMD Power Inductors*. 2009 [cit.23.6.2020]. Dostupné z: <https://www.datasheets360.com/pdf/1949640526976229294>
- [30] DUPHILY, Roland J. a spol. *Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide*. El Segundo, CA: Aerospace, Assuring Space Mission Success, 2009.
- [31] MIL-HDBK-217F_NOTICE-2. *Reliability Prediction of Electronic Equipment*. US Department of Defense, Washington DC 20301, 1995.
- [32] MIL-HDBK-338B. *Electronic Reliability Design Handbook*. US Department of Defense, Washington DC 20301, 1998.
- [33] NOAA. Satellite Technology: How big is a satellite? *National Oceanic and Atmospheric Administration* [online]. 15.9.2015 [cit. 2020-06-22]. Dostupné z: <https://www.nesdis.noaa.gov/content/satellite-technology-how-big-satellite>
- [34] O'CONNOR, Patrick a Andre KLEYNER. *Practical Reliability Engineering* [online]. 5th ed. Oxford: Wiley-Blackwell, 2012. ISBN 978-0-470-97981-5.
- [35] RAC. *Failure Mode, Effects, and Criticality Analysis (FMECA)*. Rome, NY: Reliability Analysis Center, 1993
- [36] RAC. *Worst Case Circuit Analysis Application Guidelines*. Rome, NY: Reliability Analysis Center, 1993

- [37] RIEBEEK, Holli. Catalog of Earth Satellite Orbits. *NASA Earth Observatory* [online]. 4.9.2009 [cit. 2020-06-22]. Dostupné z: <https://earthobservatory.nasa.gov/features/OrbitsCatalog>
- [38] SRC. *Worst Case Circuit Analysis (WCCA)*. Rome, NY: System Reliability Center, c2004.
- [39] SYSTEM RELIABILITY DIVISION. Reliability Engineer's Toolkit. The Rome Laboratory, 1993. Dostupné také z: <http://www.dtic.mil/docs/citations/ADA278215>
- [40] Texas Instruments [online katalogový list]. *TPS54339E*. 2012 [cit. 23.6.2020]. Dostupné z: https://www.ti.com/lit/ds/symlink/tps54339e.pdf?ts=1591708526581&ref_url=https://www.ti.com/product/TPS54339E
- [41] VISHAY [online katalogový list]. *ESCC 4001/023 Qualified High Precision*. 2019 [cit.23.6.2020]. Dostupné z: <https://www.vishay.com/docs/53037/phr.pdf>
- [42] VISHAY [online katalogový list]. *ESCC 4001/026 Qualified*. 2018 [cit.23.6.2020]. Dostupné z: <https://www.vishay.com/docs/52026/chphr.pdf>
- [43] WILD, Flint, ed. What Is a Satellite? *NASA* [online]. 7.8.2017 [cit. 2020-06-22]. Dostupné z: <https://www.nasa.gov/audience/forstudents/k-4/stories/nasa-knows/what-is-a-satellite-k4.html>
- [44] Upsat-EPS-Hardware [online]. LibreSpaceFoundation [cit. 2020-06-24]. Dostupné z: https://gitlab.com/librespacefoundation/upsat/upsat-eps-hardware/-/blob/master/eps_V6.pdf

SEZNAM OBRÁZKŮ

Obr. 1 Přehled hmotností některých satelitů	17
Obr. 2 Rozdělení disciplín podle ECSS	21
Obr. 3 Rozdělení větve spolehlivosti a bezpečnosti.....	21
Obr. 4 Odlehčení napětí keramického kondenzátoru	24
Obr. 5 Vztah pracovního zatížení a parametrů součásti.....	25
Obr. 6 Sériová struktura zapojení bloků.....	34
Obr. 7 Paralelní struktura zapojení bloků.....	34
Obr. 8 Kombinovaná struktura zapojení bloků	35
Obr. 9 Hierarchický postup FMECA analýzy	38
Obr. 10 Nebezpečí a scénář nastoupení jeho nastoupení	42
Obr. 11 Nebezpečí a scénář jeho nastoupení (Vznik více scénářů z jednoho nebezpečí).....	43
Obr. 12 Nebezpečí a scénář jeho nastoupení (Vznik jednoho důsledku z více nebezpečí)	43
Obr. 13 Možnosti eliminování a snižování nebezpečí	43
Obr. 14 Postupný proces analýzy nebezpečí.....	44
Obr. 15 Vzorový strom poruchových stavů	46
Obr. 16 Satelit UPSat	48
Obr. 17 Systémy satelitu UPSat	49
Obr. 18 Nosná konstrukce satelitu UPSat	50
Obr. 19 Základní deska EPS s bateriemi.....	51
Obr. 20 USB fotoaparát XIMEA.....	51
Obr. 21 Vědecká jednotka	52
Obr. 22 Výklopný systém antén satelitu	53
Obr. 23 Schéma analyzovaného obvodu EPS	56
Obr. 24 Křivka odlehčení napětí pro keramický kondenzátor	59
Obr. 25 Křivka odlehčení napětí pro tantalový kondenzátor	59
Obr. 26 Bezporuchovost paralelního systému pro misi ($t=1,5$ let)	65
Obr. 27 Bezporuchovost paralelního systému pro misi ($t=15$ let)	66

SEZNAM TABULEK

Tab. 1 Kategorie satelitů podle jejich hmotnosti.....	16
Tab. 2 Specifikace pravděpodobnosti splnění mise	19
Tab. 3 Základní rozdělení vojenských dokumentů	22
Tab. 4 Odlehčované parametry součástek dle typu součástek	25
Tab. 5 Ovlivnění parametrů součástek podmínkami okolí	26
Tab. 6 Typ používaných tolerančních hodnot podle ovlivňujících podmínek.....	27
Tab. 7 Příklad vlivu stárnutí na parametry	28
Tab. 8 Výpočet hodnot WCA podle metody EVA.....	28
Tab. 9 Výpočet hodnot WCA podle metody RSS.....	28
Tab. 10 Příklad ovlivněných a náhodných toleranční hodnot kondenzátoru	29
Tab. 11 Převodová tabulka úrovně kvality součástek.....	32
Tab. 12 Hodnocení závažnosti důsledků na systémové úrovni nebo úrovni satelitu.....	37
Tab. 13 Faktor závažnosti, kategorie závažnosti a úroveň závažnosti	39
Tab. 14 Pravděpodobnost výskytu poruchy a faktor pravděpodobnosti	39
Tab. 15 Matice kritičnosti	40
Tab. 16 Kategorie závažnosti nebezpečí	41
Tab. 17 Úkoly obsažené v postupných krocích analýzy nebezpečí	45
Tab. 18 Schématické značky používané pro sestavení stromu poruch	47
Tab. 19 Seznam součástek nacházejících se v analyzovaném obvodu	57
Tab. 20 Součinitel pro výpočet intenzity poruch regulátoru napětí dle MIL-HDBK-217F-2..	60
Tab. 21 Součinitele pro výpočet intenzity poruch cívk dle MIL-HDBK-217F-2	61
Tab. 22 Součinitele pro výpočet intenzity poruch tranzistoru dle MIL-HDBK-217F-2	61
Tab. 23 Součinitele pro výpočet intenzity poruch keramického kondenzátoru dle MIL-HDBK-217F-2	62
Tab. 24 Součinitele pro výpočet intenzity poruch rezistoru dle MIL-HDBK-217F-2.....	63
Tab. 25 Poměr intenzity poruch při aktivním a pasivním režimu	64
Tab. 26 Výstřižek pracovního formuláře FMECA.....	67
Tab. 27 Pravděpodobnosti způsobů poruchy	68

PŘÍLOHY

Příloha 1: Výpočet odlehčení součástek

Součástka: Integrovaný obvod – Regulátor napětí

REF	PN	Teplota pouzdra [°C]
B2	TPS54339E	70

Maximální konstrukční hodnoty dle katalogu součástky			Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1					Skutečné provozní hodnoty		
Výstupní proud [A]	Vstupní napětí [V]	Teplota přechodu [°C]	Odlehčení výstupního proudu [%]	Výstupní proud [A]	Odlehčení vstupního napětí [%]	Vstupní napětí [V]	Teplota přechodu [°C]	Výstupní proud [A]	Vstupní napětí [V]	Teplota přechodu [°C]
3	23	150	80	2,4	90	20,7	110	2	12	84,85

Výstupní proud: Odlehčená hodnota 2,4 A > Skutečná provozní hodnota 2 A ✓

Vstupní napětí: Odlehčená hodnota 20,7 V > Skutečná provozní hodnota 12 V ✓

Teplota přechodu: Odlehčená hodnota 110 °C > Skutečná provozní hodnota 84,85 °C ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástku B2 ukazuje dostatečnou rezervu.

Součástka: Integrovaný obvod – Monitor proudu

REF	PN	Teplota pouzdra [°C]
M8	5962R0924401VHA	70

Maximální konstrukční hodnoty dle katalogu součástky				Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1							Skutečné provozní hodnoty			
Výstupní proud [mA]	Výstupní napětí [V]	Napájecí napětí [V]	Teplota přechodu [°C]	Odlehčen í výstupníh o proudu [%]	Výstup ní proud [mA]	Odlehčení vstupního napětí [%]	Vstup ní napět í [V]	Odlehčen í napájecí ho napětí [%]	Napáje cí napětí [V]	Teplota přechod u [°C]	Výstup ní proud [mA]	Vstup ní napětí [V]	Napájecí napětí [V]	Teplota přechod u [°C]
0,5	0,5	68	150	80	0,4	70	0,35	90	61,2	110	0,1	0,1	12	72,11

Výstupní proud: Odlehčená hodnota 0,4 mA > Skutečná provozní hodnota 0,1 mA ✓

Vstupní napětí: Odlehčená hodnota 0,35 V > Skutečná provozní hodnota 0,1 V ✓

Napájecí napětí: Odlehčená hodnota 61,2 V > Skutečná provozní hodnota 12 V ✓

Teplota přechodu: Odlehčená hodnota 110 °C > Skutečná provozní hodnota 72,11 °C ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástku M8 ukazuje dostatečnou rezervu.

Součástka: Cívka 4,3uH

REF	PN
L10	320100905C4L3M

Maximální konstrukční hodnoty dle katalogu součástky		Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1			Skutečné provozní hodnoty	
Napětí [V]	Teplota Hot Spot [°C]	Odlehčení napětí [%]	Napětí [V]	Teplota Hot Spot [°C]	Napětí [V]	Teplota Hot Spot [°C]
150	125	50	75	105	12	90,48

Napětí: Odlehčená hodnota 75 V > Skutečná provozní hodnota 12 V ✓

Teplota Hot Spot: Odlehčená hodnota 105 °C > Skutečná provozní hodnota 90,48 °C ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástku L10 ukazuje dostatečnou rezervu.

Součástka: Tranzistor FET, PMOS

REF	PN	Teplota pouzdra [°C]	Maximální konstrukční hodnoty dle katalogu součástky				
			Ztrátový výkon [W]	Výstupní proud [A]	Napětí mezi G a S [V]	Napětí mezi D a S [V]	Teplota přechodu [°C]
Q2a, Q2b	JANSR2N7519U3	70	75	18	20	30	150
Q3a, Q3b	JANSR2N7519U3	70	75	18	20	30	150
Q5a, Q5b	JANSR2N7519U3	70	75	18	20	30	150
Q7a, Q7b	JANSR2N7519U3	70	75	18	20	30	150

REF	Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1									Skutečné provozní hodnoty				
	Odlehčení ztrátového výkonu	Ztrátový výkon	Odlehčení výstupního proudu	Výstupní proud	Odlehčení napětí mezi G a S	Napětí mezi G a S	Odlehčení napětí mezi D a S	Napětí mezi D a S	Teplota přechodu	Ztrátový výkon	Výstupní proud	Napětí mezi G a S	Napětí mezi D a S	Teplota přechodu [°C]
	[%]	[W]	[%]	[A]	[%]	[V]	[%]	[V]	[°C]	[W]	[A]	[V]	[V]	[°C]
Q2a, Q2b	65	49	75	14	75	15	80	24	110	0,088	1	3,3	3,3	71,75
Q3a, Q3b	65	49	75	14	75	15	80	24	110	0,022	0,5	3,3	3,3	70,44
Q5a, Q5b	65	49	75	14	75	15	80	24	110	0,049	0,75	3,3	3,3	70,98
Q7a, Q7b	65	49	75	14	75	15	80	24	110	0,005	0,25	3,3	3,3	70,11

Ztrátový výkon: Odlehčená hodnota 49W > Skutečná provozní hodnota 0,088 (resp. 0,022; 0,049; 0,005) W ✓

Výstupní proud: Odlehčená hodnota 14 A > Skutečná provozní hodnota 1 (resp. 0,5; 0,75; 0,25) A ✓

Napětí mezi Gate a Source: Odlehčená hodnota 15 V > Skutečná provozní hodnota 3,3 V ✓

Napětí mezi Drain a Source: Odlehčená hodnota 24 V > Skutečná provozní hodnota 3,3 V ✓

Teplota přechodu: Odlehčená hodnota 110 °C > Skutečná provozní hodnota 71,75 °C ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástky Q2a, Q2b, Q3a, Q3b, Q5a, Q5b, Q7a Q7b ukazuje dostatečnou rezervu.

Součástka: Keramický kondenzátor

REF	El. kapacita	PN	Teplota pouzdra [°C]
C43	10nF	300904103103KC	70
C38	100nF	300904103104KC	70
C44	100nF	300904103104KC	70
C85	1uF	300904103105KA	70
C84	1uF	300904103105KA	70
C79	10uF	300904103106KX	70
C41	10uF	300904103106KX	70
C37	10uF	300904103106KX	70
C50	10uF	300904103106KX	70
C56	10uF	300904103106KX	70
C59	10uF	300904103106KX	70

	Maximální konstrukční hodnoty dle katalogu součástky	Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1		Skutečné provozní hodnoty
REF	Napětí [V]	Odlehčení napětí [%]	Napětí [V]	Napětí [V]
C43	50	60	30	12
C38	50	60	30	5,7
C44	50	60	30	5,7
C85	25	60	15	3,3
C84	25	60	15	3,3
C79	16	60	9,6	3,3
C41	16	60	9,6	3,3
C37	16	60	9,6	3,3
C50	16	60	9,6	3,3
C56	16	60	9,6	3,3
C59	16	60	9,6	3,3

Napětí: Odlehčené hodnoty všech kondenzátorů > skutečné provozní hodnoty ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástky C43, C38, C44, C85, C84, C79, C41, C37, C50, C56, C59 ukazuje dostatečnou rezervu.

Součástka: Tantalový kondenzátor

REF	Value	PN	Teplota pouzdra [°C]	Maximální konstrukční hodnoty dle katalogu součástky		
				Napětí [V]	Nárazový proud [A]	Zvlnění proudu [A]
C71	100uF	301200102C107AK	70	10	7,14	0,944
C72	100uF	301200102C107AK	70	10	7,14	0,944
C73	100uF	301200102C107AK	70	10	7,14	0,944
C87	100uF	301200102C107AK	70	10	7,14	0,944

REF	Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev. 1						Skutečné hodnoty		
	Odlehčení napětí [%]	Napětí [V]	Odlehčení nárazového proudu [%]	Nárazový proud [A]	Odlehčení zvlnění proudu [%]	Zvlnění proudu [A]	Napětí [V]	Nárazový proud [A]	Zvlnění proudu [A]
C71	60	6	75	5,36	50	0,472	3,3	2,36	0,243
C72	60	6	75	5,36	50	0,472	3,3	2,36	0,243
C73	60	6	75	5,36	50	0,472	3,3	2,36	0,243
C87	60	6	75	5,36	50	0,472	3,3	2,36	0,243

Napětí: Odlehčená hodnota 6 V > Skutečná provozní hodnota 3,3 V ✓

Nárazový proud: Odlehčená hodnota 5,36 A > Skutečná provozní hodnota 2,36 A ✓

Zvlnění proudu: Odlehčená hodnota 0,472 A > Skutečná provozní hodnota 0,243 V ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástky C71, C72, C73 a C87 ukazuje dostatečnou rezervu.

Součástka: Rezistor

				Maximální konstrukční hodnoty dle katalogu součástky	
REF	El. odpor [Ohm]	PN	Teplota pouzdra [°C]	Napětí [V]	Výkon [W]
RFB3	73200	4001023027322B2	70	150	0,125
RFB4	22100	4001023022212B2	70	150	0,125
R44	1000	4001026021001F4	70	150	0,2
R39	20000	4001026022002F4	70	150	0,2
R52	56000	4001026025602F4	70	150	0,2
R56	18	40010260218R0F4	70	150	0,2
R41	18	40010260218R0F4	70	150	0,2
R42	18	40010260218R0F4	70	150	0,2
R64	18	40010260218R0F4	70	150	0,2
R40	0,05	400102701R050D	70	0,316	1

	Odlehčené hodnoty dle ECSS-Q-ST-30-11C Rev 1				Skutečné hodnoty	
REF	Odlehčení napětí [%]	Napětí [V]	Odlehčení výkonu [%]	Výkon [W]	Napětí [V]	Výkon [W]
RFB3	80	120	50	0,0625	2,53	8,78E-05
RFB4	80	120	50	0,0625	0,77	2,65E-05
R44	80	120	50	0,1	0	0
R39	80	120	50	0,1	2	2,00E-04
R52	80	120	50	0,1	3,3	1,94E-04
R56	80	120	50	0,1	0	0
R41	80	120	50	0,1	0	0
R42	80	120	50	0,1	0	0
R64	80	120	50	0,1	0	0
R40	80	0,2528	50	0,5	0,1	0,2

Napětí: Odlehčené hodnoty všech rezistorů > skutečné provozní hodnoty ✓

Výkon: Odlehčené hodnoty všech rezistorů > skutečné provozní hodnoty ✓

Všechny podmínky byly splněny, analýza odlehčení pro součástky RFB3, RFB4, R44, R39, R52, R56, R41, R42, R64 a R40 ukazuje dostatečnou rezervu.

Příloha 2: Výpočet intenzit poruch

Ref. Číslo	Součástka	PN	Hodnota	Rating	Teplota pouzdra [°C]	Teplota přechodu [°C]	Elektrické zatížení	Stress [-]	Třída součástky
B2	Integrovaný obvod, Regulátor napětí	TPS54339E			70	84,85			-
M8	Integrovaný obvod, Monitor proudu	5962R0924401VHA			70	72,11			Class V
L10	Cívka, 4,3 µH, SMD	320100905C4L3M			70	90,48			ESCC C
Q2a	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	71,75			JANS
Q3a	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,44			JANS
Q5a	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,98			JANS
Q7a	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,11			JANS
Q2b	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	71,75			JANS
Q3b	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,44			JANS
Q5b	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,98			JANS
Q7b	Tranzistor FET, PMOS, 30 V, 75 W	JANSR2N7519U3			70	70,11			JANS
C43	Kondenzátor, Keramický, 10 nF, 10 %, 50 V	300904103103KC	0.01 uF	50 V	70		12 V	0,240	ESCC C

Ref. Číslo	C1	C2	λb [za milion hodin]	πT	πV	πC	πS	πP	πA	πSR	πE	πQ	πL	λOP [za hodinu]	λNOP [za hodinu]
B2	0,01	0,0013		6,90							0,5	1	1	6,962E-08	6,962E-09
M8	0,01	0,0020		3,17							0,5	0,25	1	8,165E-09	8,165E-10
L10			0,00003	2,16							0,5	0,3		9,735E-12	4,868E-12
Q2a			0,012	2,40					0,7		0,5	0,7		7,060E-09	1,412E-09
Q3a			0,012	2,35					0,7		0,5	0,7		6,911E-09	1,382E-09
Q5a			0,012	2,37					0,7		0,5	0,7		6,972E-09	1,394E-09
Q7a			0,012	2,34					0,7		0,5	0,7		6,874E-09	1,375E-09
Q2b			0,012	2,40					0,7		0,5	0,7		7,060E-09	1,412E-09
Q3b			0,012	2,35					0,7		0,5	0,7		6,911E-09	1,382E-09
Q5b			0,012	2,37					0,7		0,5	0,7		6,972E-09	1,394E-09
Q7b			0,012	2,34					0,7		0,5	0,7		6,874E-09	1,375E-09
C43			0,002	5,98	1,064	0,661				1	0,5	0,3		1,261E-09	2,522E-10

Ref. Číslo	Součástka	PN	Hodnota	Rating	Teplota pouzdra [°C]	Teplota přechodu [°C]	Elektrické zatížení	Stress [-]	Třída součástky
C38	Kondenzátor, Keramický, 100 nF, 10 %, 50 V	300904103104KC	0.1 uF	50 V	70		5,7 V	0,114	ESCC C
C44	Kondenzátor, Keramický, 100 nF, 10 %, 50 V	300904103104KC	0.1 uF	50 V	70		5,7 V	0,114	ESCC C
C85	Kondenzátor, Keramický, 1 uF, 10 %, 25 V	300904103105KA	1 uF	25 V	70		3,3 V	0,132	ESCC C
C84	Kondenzátor, Keramický, 1 uF, 10 %, 25 V	300904103105KA	1 uF	25 V	70		3,3 V	0,132	ESCC C
C79	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C41	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C37	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C50	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C56	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C59	Kondenzátor, Keramický, 10 uF, 10 %, 16 V	300904103106KX	10 uF	16 V	70		3,3 V	0,206	ESCC C
C71	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK	100 uF	10 V	70		3,3 V	0,330	ESCC C

Ref. Číslo	C1	C2	λb [za milion hodin]	πT	πV	πC	πS	πP	πA	πSR	πE	πQ	πL	λOP [za hodinu]	λNOP [za hodinu]
C38			0,002	5,98	1,007	0,813				1	0,5	0,3		1,468E-09	2,936E-10
C44			0,002	5,98	1,007	0,813				1	0,5	0,3		1,468E-09	2,936E-10
C85			0,002	5,98	1,011	1,000				1	0,5	0,3		1,813E-09	3,625E-10
C84			0,002	5,98	1,011	1,000				1	0,5	0,3		1,813E-09	3,625E-10
C79			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C41			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C37			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C50			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C56			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C59			0,002	5,98	1,041	1,230				1	0,5	0,3		2,296E-09	4,592E-10
C71			0,00005	2,15	1,000	2,884				3,3	0,5	0,3		1,536E-10	3,072E-11

Ref. Číslo	Součástka	PN	Hodnota	Rating	Teplota pouzdra [°C]	Teplota přechodu [°C]	Elektrické zatížení	Stress [-]	Třída součástky
C72	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK	100 uF	10 V	70		3,3 V	0,330	ESCC C
C73	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK	100 uF	10 V	70		3,3 V	0,330	ESCC C
C87	Kondenzátor, Tantalový, 100 uF, 10 %, 10 V	301200102C107AK	100 uF	10 V	70		3,3 V	0,330	ESCC C
RFB3	Film rezistor, 73.2 kOhm, 0.125 W	4001023027322B2	73200 Ohm	0.125 W	70		0.00009 W		ESCC C
RFB4	Film rezistor, 22.1 kOhm, 0.125 W	4001023022212B2	22100 Ohm	0.125 W	70		0.00003 W		ESCC C
R44	Film rezistor, 1 kOhm, 0.2 W	4001026021001F4	1000 Ohm	0.2 W	70		0 W		ESCC C
R39	Film rezistor, 20 kOhm, 0.2 W	4001026022002F4	20000 Ohm	0.2 W	70		0.00020 W		ESCC C
R52	Film rezistor, 56 kOhm, 0.2 W	4001026025602F4	56000 Ohm	0.2 W	70		0.00019 W		ESCC C
R56	Film rezistor, 18 Ohm, 0.2 W	40010260218R0F4	18 Ohm	0.2 W	70		0 W		ESCC C
R41	Film rezistor, 18 Ohm, 0.2 W	40010260218R0F4	18 Ohm	0.2 W	70		0 W		ESCC C
R42	Film rezistor, 18 Ohm, 0.2 W	40010260218R0F4	18 Ohm	0.2 W	70		0 W		ESCC C
R64	Film rezistor, 18 Ohm, 0.2 W	40010260218R0F4	18 Ohm	0.2 W	70		0 W		ESCC C
R40	Film rezistor, 0.05 Ohm, 2 W	400102701R050D	0.05 Ohm	1 W	70		0.2 W		ESCC C

Ref. Číslo	C1	C2	λb [za milion hodin]	πT	πV	πC	πS	πP	πA	πSR	πE	πQ	πL	λOP [za hodinu]	λNOP [za hodinu]
C72			0,00005	2,15	1,000	2,884				3,3	0,5	0,3		1,536E-10	3,072E-11
C73			0,00005	2,15	1,000	2,884				3,3	0,5	0,3		1,536E-10	3,072E-11
C87			0,00005	2,15	1,000	2,884				3,3	0,5	0,3		1,536E-10	3,072E-11
RFB3			0,0037	1,50			0,79	0,444			0,5	0,3		2,932E-10	1,466E-10
RFB4			0,0037	1,50			0,79	0,444			0,5	0,3		2,932E-10	1,466E-10
R44			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R39			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R52			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R56			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R41			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R42			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R64			0,0037	1,50			0,79	0,534			0,5	0,3		3,522E-10	1,761E-10
R40			0,0037	1,50			0,88	1,000			0,5	0,3		7,389E-10	3,695E-10

Příloha 3: FMECA

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM1	B2	Regulátor napětí, step-down, 3,3V	Ztráta výstupu	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,52	1,00	3,620E-08	4,76E-04	2	6
FM2	B2	Regulátor napětí, step-down, 3,3V	Podpětí na výstupu	Napětí na výstupu z měniče B2 klesne pod nominální hodnotu 3,3V.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,48	0,50	1,671E-08	2,20E-04	2	6
FM3	B2	Regulátor napětí, step-down, 3,3V	Přepětí na výstupu	Napětí na výstupu z měniče B2 vyroste nad nominální hodnotu (v nejhorším možném případě až 12V).	Fyzické poškození desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná		0,50	1,671E-08	2,20E-04	2	6
FM4	M8	Monitor proudu	Ztráta výstupu	Nepřipojeno.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,52	1,00	4,246E-09	5,58E-05	2	2
FM5			Nesprávný výstup	Nepřipojeno.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,48	1,00	3,919E-0	5,15E-05	2	2

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM6	RFB3	Film rezistor 73,2k Ω	Přerušení	Nulové napětí na vstupu do zpětné vazby B2, výstup z měniče vyroste na 12V.	Fyzické poškození desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	2,932E-10	3,85E-06	1	3
FM7	RFB4	Film rezistor 22,1k Ω	Přerušení	3,3V na vstupu do zpětné vazby B2, výstup z regulátoru poklesne na hodnotu referenčního napětí.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	2,932E-10	3,85E-06	1	3
FM8	R39	Film rezistor 2k Ω	Přerušení	Nepřipojeno.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	1
FM9	R40	Rezistor pro měření proudu	Přerušení	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	7,389E-10	9,71E-06	1	3
FM10	R41	Film rezistor 2,7 Ω	Přerušení	Nulové napětí na elektrodě G tranzistorů Q2a, 2b.	Ztráta napájení desky COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	3
FM11	R42	Film rezistor 2,7 Ω	Přerušení	Nulové napětí na elektrodě G tranzistorů Q3a, Q3b.	Nepřipojeno. Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	1

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM12	R44	Film rezistor 1k Ω	Přerušení	Nulové napětí na pinu 7. Ztráta regulovaného napětí na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	3
FM13	R56	Film rezistor 2,7 Ω	Přerušení	Nulové napětí na elektrodě G tranzistorů Q5a, Q5b	Ztráta napájení desky OBC.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	3
FM14	R52	Film rezistor 1k Ω	Přerušení	Možná nestabilita a kmitání v případě změny stavu na elektrodě G tranzistorů Q2a, Q2b.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	1
FM15	R64	Film rezistor 2,7 Ω	Přerušení	Nulové napětí na elektrodě G tranzistorů Q7a, Q7b.	Nepřipojeno. Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	1,00	1,00	3,522E-10	4,63E-06	1	1
FM16	C37	Keramický kondenzátor 10 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z tranzistorů Q5a, Q5b.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2
FM17	C37	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																	
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020							
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka							
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN	
FM18	C38	Keramický kondenzátor 0,1 μ F	Přerušení	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,37	1,00	5,431E-10	7,14E-06	1	3	
FM19	C38	Keramický kondenzátor 0,1 μ F	Zkrat	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,248E-10	1,22E-05	2	6	
FM20	C41	Keramický kondenzátor 10 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2	
FM21	C41	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6	
FM22	C43	Keramický kondenzátor 10 μ F	Přerušení	Nesprávná funkce soft start při náběhu měniče B2.	Možné zvýšené proudové zatížení a rušení komponent na deskách OBC a COMM.	Nesprávná funkce satelitu	3SP	2	Nesprávná nebo ztráta komunikace se satelitem	Žádná	0,37	1,00	4,665E-10	6,13E-06	1	2	

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM23	C43	Keramický kondenzátor 10 μ F	Zkrat	Pin 8 je zkratován k zemi. Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	7,943E-10	1,04E-05	2	6
FM24	C44	Keramický kondenzátor 0,1 μ F	Přerušení	Možná nesprávná regulace nebo zákmity napětí na výstupu z regulátoru B2.	Možné nesprávné napětí desek OBC a COMM.	Nesprávná funkce satelitu	3SP	2	Nesprávná nebo ztráta komunikace se satelitem	Žádná	0,37	1,00	5,431E-10	7,14E-06	1	2
FM25	C44	Keramický kondenzátor 0,1 μ F	Zkrat	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,248E-10	1,22E-05	2	6
FM26	C50	Keramický kondenzátor 10 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z tranzistorů Q2a, Q2b.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2
FM27	C50	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6
FM28	C56	Keramický kondenzátor 10 μ F	Přerušení	Přerušení kondenzátoru C56.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM29	C56	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6
FM30	C59	Keramický kondenzátor 10 μ F	Přerušení	Přerušení kondenzátoru C59.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2
FM31	C59	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6
FM32	C71	Tantalový kondenzátor 100 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	5,684E-11	7,47E-07	1	1
FM33	C71	Tantalový kondenzátor 100 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,677E-11	1,27E-06	1	3
FM34	C72	Tantalový kondenzátor 100 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Ztráta komunikace se satelitem	Žádná	0,37	1,00	5,684E-11	7,47E-07	1	1

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM35	C72	Tantalový kondenzátor 100 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,677E-11	1,27E-06	1	3
FM36	C73	Tantalový kondenzátor 100 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	5,684E-11	7,47E-07	1	1
FM37	C73	Tantalový kondenzátor 100 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,677E-11	1,27E-06	1	3
FM38	C79	Keramický kondenzátor 10 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	8,496E-10	1,12E-05	2	2
FM39	C79	Keramický kondenzátor 10 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,447E-09	1,90E-05	2	6
FM40	C84	Keramický kondenzátor 1 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	6,707E-10	8,81E-06	1	1

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součástí	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM41	C84	Keramický kondenzátor 1 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,142E-09	1,50E-05	2	6
FM42	C85	Keramický kondenzátor 1 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	6,707E-10	8,81E-06	1	1
FM43	C85	Keramický kondenzátor 1 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	1,142E-09	1,50E-05	2	6
FM44	C87	Tantalový kondenzátor 100 μ F	Přerušení	Možné mírné zvlnění napětí na výstupu z měniče B2.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,37	1,00	5,684E-11	7,47E-07	1	1
FM45	C87	Tantalový kondenzátor 100 μ F	Zkrat	Výstup z měniče B2 je zkratován k zemi. Nadproudová ochrana odpojí trvale výstup z měniče.	Ztráta napájení desek OBC a COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,63	1,00	9,677E-11	1,27E-06	1	3

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM46	Q2a	Tranzistor FET, PMOS	Přerušení	Zvýšení proudu tekoucího tranzistorem Q5a a jeho možné poškození.	Pravděpodobná ztráta napájení desky COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,27	1,00	1,906E-09	2,50E-05	2	6
FM47	Q2a	Tranzistor FET, PMOS	Zkrat	Tranzistor Q2a zůstane trvale připojen.	Ztráta funkce spínání desky COM.	Degradace vnitřní funkce satelitu.	3SP	2	Žádná	Žádná	0,73	1,00	5,153E-09	6,77E-05	2	4
FM48	Q2b	Tranzistor FET, PMOS	Přerušení	Zvýšení proudu tekoucího tranzistorem Q5a a jeho možné poškození.	Pravděpodobná ztráta napájení desky COMM.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,27	1,00	1,906E-09	2,50E-05	2	6
FM49	Q2b	Tranzistor FET, PMOS	Zkrat	Tranzistor Q2a zůstane trvale připojen.	Ztráta funkce spínání desky COM.	Degradace vnitřní funkce satelitu.	3SP	2	Žádná	Žádná	0,73	1,00	5,153E-09	6,77E-05	2	4
FM50	Q3a	Tranzistor FET, PMOS	Přerušení	Tranzistorem Q3b neteče žádný proud.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,27	1,00	1,866E-09	2,45E-05	2	2
FM51	Q3a	Tranzistor FET, PMOS	Zkrat	Tranzistor Q3a zůstane trvale připojen.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,73	1,00	5,045E-09	6,63E-05	2	2

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompensace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM52	Q3b	Tranzistor FET, PMOS	Přerušení	Tranzistorem Q3a neteče žádný proud.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,27	1,00	1,866E-09	2,45E-05	2	2
FM53	Q3b	Tranzistor FET, PMOS	Zkrat	Tranzistor Q3b zůstane trvale připojen.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,73	1,00	5,045E-09	6,63E-05	2	2
FM54	Q5a	Tranzistor FET, PMOS	Přerušení	Zvýšení proudu tekoucího tranzistorem Q5b a jeho možné poškození.	Pravděpodobná ztráta napájení desky OBC.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,27	1,00	1,882E-09	2,47E-05	2	6
FM55	Q5a	Tranzistor FET, PMOS	Zkrat	Tranzistor Q5a zůstane trvale připojen.	Ztráta funkce spínání desky OBC.	Degradace vnitřní funkce satelitu.	3SP	2	Žádná	Žádná	0,73	1,00	5,089E-09	6,69E-05	2	4
FM56	Q5b	Tranzistor FET, PMOS	Přerušení	Zvýšení proudu tekoucího tranzistorem Q5a a jeho možné poškození.	Pravděpodobná ztráta napájení desky OBC.	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,27	1,00	1,882E-09	2,47E-05	2	6
FM57	Q5b	Tranzistor FET, PMOS	Zkrat	Tranzistor Q5b zůstane trvale připojen.	Ztráta funkce spínání desky OBC.	Degradace vnitřní funkce satelitu.	3SP	2	Žádná	Žádná	0,73	1,00	5,089E-09	6,69E-05	2	4

Analýza způsobů, důsledků a kritičnosti poruch (FMECA)																
Produkt: satelit UPSat				Popis funkce: Regulace napětí +3,3 VDC						Datum vypracování: 16.5.2020						
Modul: elektrický zdrojový systém (EPS)				Délka mise: 18 měsíců (13140 h), LEO						Vypracoval: Marek Horčíčka						
FM. ID	Ref. číslo	Popis součásti	Způsob poruchy	Lokální důsledek	Důsledek na další úrovni	Konečný důsledek	Úroveň závažnosti	SN	Detekce nebo projev poruchy	Kompenzace poruchy	Pravd. způsobu poruchy α	Pravd. Důsledků poruchy β	Intenzita způsobu poruchy λ_{fm} (1/h)	Pravděpodobnost způsobu poruchy	PN	CN
FM58	Q7a	Tranzistor FET, PMOS	Přerušení	Tranzistorem Q7b neteče žádný proud.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,27	1,00	1,856E-09	2,44E-05	2	2
FM59	Q7a	Tranzistor FET, PMOS	Zkrat	Tranzistor Q7a zůstane trvale připojen.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,73	1,00	5,018E-09	6,59E-05	2	2
FM60	Q7b	Tranzistor FET, PMOS	Přerušení	Tranzistorem Q7a neteče žádný proud.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,27	1,00	1,856E-09	2,44E-05	2	2
FM61	Q7b	Tranzistor FET, PMOS	Zkrat	Tranzistor Q7b zůstane trvale připojen.	Nemá vliv na normální funkci.	Bez vlivu na funkci.	4SP	1	Žádná	Žádná	0,73	1,00	5,018E-09	6,59E-05	2	2
FM62	L10	Cívka 4,7 μ H	Přerušení	Ztráta regulovaného napětí 3,3V na výstupu z měniče B2.	Ztráta napájení desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,50	1,00	4,868E-12	6,40E-08	1	3
FM63	L10	Cívka 4,7 μ H	Zkrat	Přepětí na výstupu z měniče B2.	Fyzické poškození desek OBC a COMM	Ztráta funkce satelitu	2SP	3	Ztráta komunikace se satelitem	Žádná	0,50	1,00	4,868E-12	6,40E-08	1	3